QoS: Policing and Shaping Configuration Guide, Cisco IOS XE Release 2

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

Policing and Shaping Overview

Cisco IOS XE QoS offers two kinds of traffic regulation mechanisms--policing and shaping.

You can deploy these traffic regulation mechanisms (referred to as policers and shapers) throughout your network to ensure that a packet, or data source, adheres to a stipulated contract and to determine the QoS to render the packet. Both policing and shaping mechanisms use the traffic descriptor for a packet--indicated by the classification of the packet--to ensure adherence and service.

Policers and shapers usually identify traffic descriptor violations in an identical manner. They usually differ, however, in the way they respond to violations, for example:

- A policer typically drops traffic, but it can also change the setting or "marking" of a packet. (For example, a policer will either drop the packet or rewrite its IP precedence, resetting the type of service bits in the packet header.)
- A shaper typically delays excess traffic using a buffer, or queueing mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected. (For example, Class-Based Shaping uses a weighted fair queue to delay packets in order to shape the flow.)

Traffic shaping and policing can work in tandem. For example, a good traffic shaping scheme should make it easy for nodes inside the network to detect misbehaving flows. This activity is sometimes called policing the traffic of the flow.

This chapter gives a brief description of the Cisco IOS XE QoS traffic policing and shaping mechanisms. Because policing and shaping both use the token bucket mechanism, this chapter first explains how a token bucket works. This chapter includes the following sections:

What Is a Token Bucket

A token bucket is a formal definition of a rate of transfer. It has three components: a burst size, a mean rate, and a time interval (Tc). Although the mean rate is generally represented as bits per second, any two values may be derived from the third by the relation shown as follows:

```
mean rate = burst size / time interval
```

Here are some definitions of these terms:

- Mean rate--Also called the committed information rate (CIR), it specifies how much data can be sent or forwarded per unit time on average.

- Burst size--Also called the Committed Burst (Bc) size, it specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns. (For a shaper, it specifies bits per burst; for a policer, it specifies bytes per burst.)
- Time interval--Also called the measurement interval, it specifies the time quantum in seconds per burst.

By definition, over any integral multiple of the interval, the bit rate of the interface will not exceed the mean rate. The bit rate, however, may be arbitrarily fast within the interval.

A token bucket is used to manage a device that regulates the data in a flow. For example, the regulator might be a traffic policer or a traffic shaper. A token bucket itself has no discard or priority policy. Rather, a token bucket discards tokens and leaves to the flow the problem of managing its transmission queue if the flow overdrives the regulator.

In the token bucket metaphor, tokens are put into the bucket at a certain rate. The bucket itself has a specified capacity. If the bucket fills to capacity, newly arriving tokens are discarded. Each token is permission for the source to send a certain number of bits into the network. To send a packet, the regulator must remove from the bucket a number of tokens equal in representation to the packet size.

If not enough tokens are in the bucket to send a packet, the packet either waits until the bucket has enough tokens or is discarded or marked down. If the bucket is already full of tokens, incoming tokens overflow and are not available to future packets. Thus, at any time, the largest burst a source can send into the network is roughly proportional to the size of the bucket.

Note that the token bucket mechanism that is used for traffic shaping has both a token bucket and a data buffer, or queue; if it did not have a data buffer, it would be a policer. For traffic shaping, packets that arrive that cannot be sent immediately are delayed in the data buffer.

For traffic shaping, a token bucket permits burstiness but bounds it. It guarantees that the burstiness is bounded so that the flow will never send faster than the token bucket’s capacity, divided by the time interval, plus the established rate at which tokens are placed in the token bucket. See the following formula:

```
(token bucket capacity in bits / time interval in seconds) + established rate in bps =
maximum flow speed in bps
```

This method of bounding burstiness also guarantees that the long-term transmission rate will not exceed the established rate at which tokens are placed in the bucket.

Traffic Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or class of service (CoS).

Traffic policing manages the maximum rate of traffic through a token bucket algorithm. The token bucket algorithm can use the user-configured values to determine the maximum rate of traffic allowed on an interface at a given moment in time. The token bucket algorithm is affected by all traffic entering or leaving (depending on where the traffic policy with traffic policing is configured) and is useful in managing network bandwidth when several large packets are sent in the same traffic stream.

The token bucket algorithm provides users with three actions for each packet: a conform action, an exceed action, and an optional violate action. Traffic that is entering the interface with Traffic Policing configured is placed in to one of these categories. Within these three categories, users can decide packet treatments. For instance, packets that conform can be configured to be transmitted, packets that exceed can be configured to be sent with a decreased priority, and packets that violate can be configured to be dropped.

Traffic policing is often configured on interfaces at the edge of a network to limit the rate of traffic that is entering or leaving the network. In the most common traffic policing configurations, traffic that conforms is transmitted and traffic that exceeds is sent with a decreased priority or is dropped. Users can change these configuration options to suit their network needs.

Traffic Shaping to Regulate Packet Flow

Regulating the packet flow (that is, the flow of traffic) on the network is also known as traffic shaping. Traffic shaping allows you to control the speed of traffic that is leaving an interface. This way, you can match the flow of the traffic to the speed of the interface receiving the packet.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Distribution of Remaining Bandwidth Using Ratio

The Distribution of Remaining Bandwidth Using Ratio feature allows service providers to configure a bandwidth-remaining ratio on subinterfaces and class queues. This ratio specifies the relative weight of a subinterface or queue with respect to other subinterfaces or queues. During congestion, the router uses this bandwidth-remaining ratio to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class of nonpriority traffic. The router allocates excess bandwidth relative to the other subinterface-level queues and class queues configured on the physical interface. By administration of a bandwidth-remaining ratio, traffic priority is not based solely on speed. Instead, the service provider can base priority on alternative factors such as service product and subscription rate.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Distribution of Remaining Bandwidth Using Ratio

Before enabling the Distribution of Remaining Bandwidth Using Ratio feature, create as many traffic classes as you need by using the class-map command.

Restrictions for Distribution of Remaining Bandwidth Using Ratio

- Bandwidth-remaining ratios can be used on outbound interfaces only.
- The bandwidth remaining ratio command cannot coexist with another bandwidth command in different traffic classes of the same policy map. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth remaining ratio 10
 class precedence_2
  bandwidth 1000
```

- The bandwidth remaining ratio command cannot coexist with another bandwidth command in the same class. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth 1000
  bandwidth remaining ratio 10
```

- The bandwidth remaining ratio command cannot coexist with the priority command in the same class. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_1
  priority percent 10
  bandwidth remaining ratio 10
```

Information About Distribution of Remaining Bandwidth Using Ratio

- Benefits of the Distribution of Remaining Bandwidth Using Ratio Feature, page 6
- Bandwidth-Remaining Ratio Functionality, page 7

Benefits of the Distribution of Remaining Bandwidth Using Ratio Feature

The Distribution of Remaining Bandwidth Using Ratio feature allows service providers to prioritize subscriber traffic during periods of congestion. A bandwidth-remaining ratio is used to influence how the router allocates excess bandwidth (unused by priority traffic) to a class of nonpriority traffic. Instead of using only bandwidth rate, the router considers configured minimum bandwidth rates, maximum bandwidth rates, and bandwidth-remaining ratios when determining excess bandwidth allocation. A bandwidth-remaining ratio adds more flexibility in prioritizing traffic and enables you to influence excess bandwidth allocation by basing the bandwidth-remaining ratio on factors other than speed.

With bandwidth-remaining ratios, service providers have more flexibility in assigning priority to subinterfaces and queues during congestion. In addition to speed, you can base the bandwidth-remaining ratio on alternative factors, such as a service product or subscription rate. In this way, for example, you can give higher weight to subinterfaces that carry business services and lower weight to subinterfaces that carry residential services.

Bandwidth-Remaining Ratio Functionality

A bandwidth-remaining ratio, specified by the **bandwidth remaining ratio** command, is a value from 1 to 1000 that is used to determine the amount of unused (excess) bandwidth to allocate to a class-level queue or subinterface-level queue during congestion. The router allocates the excess bandwidth relative to the other class-level queues and subinterface-level queues configured on the physical interface. The bandwidth-remaining ratio value does not indicate a percentage. As the name implies, a ratio is used. For example, a subinterface with a bandwidth-remaining ratio of 100 receives 10 times the unused (excess) bandwidth during congestion than a subinterface with a bandwidth-remaining ratio of 10.

Without bandwidth-remaining ratios, the queueing mechanism or scheduler on the router allocates unused (excess) bandwidth equally among the classes or subinterfaces.

With bandwidth-remaining ratios, unused (excess) bandwidth allocation can be based on factors other than the bandwidth rate (for example, the service product or the subscription rate).

Using the bandwidth remaining ratio command, the bandwidth-remaining ratio can be configured differently on each subinterface or class. The bandwidth-remaining ratio can range from 1 to 1000. For example, if there are three subscribers, and the bandwidth-remaining ratios are configured as 9, 7, and 1, and if after priority traffic is served, there are 1700 kbps of excess bandwidth, the subscribers get 900 kbps, 700 kbps, and 100 kbps, respectively.

How to Configure Distribution of Remaining Bandwidth Using Ratio

You can apply bandwidth-remaining ratios to subinterfaces and/or classes queues.

- Configuring and Applying Bandwidth-Remaining Ratios to Subinterfaces, page 7
- Configuring and Applying Bandwidth-Remaining Ratios to Class Queues, page 12

Configuring and Applying Bandwidth-Remaining Ratios to Subinterfaces

Note You can apply bandwidth-remaining ratios to outbound subinterfaces only.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *child-policy-name*
4. **class** *class-map-name*
5. **bandwidth** *bandwidth-kbps*
6. Repeat Steps Configuring and Applying Bandwidth-Remaining Ratios to Subinterfaces, page 7 and Configuring and Applying Bandwidth-Remaining Ratios to Subinterfaces, page 7 to configure additional traffic classes, if needed.
7. **exit**
8. **exit**
9. **policy-map** *parent-policy-name*
10. **class class-default**
11. **bandwidth remaining ratio** *ratio*
12. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
13. **service-policy** *child-policy-name*
14. **exit**
15. **exit**
16. **interface** *type slot* / *module* / *port* **.** *subinterface* [**point-to-point** | **multipoint**]
17. **service-policy output** *parent-policy-name*
18. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *child-policy-name* **Example:** `Router(config)# policy-map Child`	Creates or modifies a child policy map and enters policy-map configuration mode. • Enter the name of the child policy map.

	Command or Action	Purpose

Step 4	**class** *class-map-name*
	Example:
	`Router(config-pmap)# class precedence_0`
		Configures the class map and enters policy-map class configuration mode.

Step 5	**bandwidth** *bandwidth-kbps* **Example:** `Router(config-pmap-c)# bandwidth 10000`	Specifies the bandwidth, in kbps, to be allocated to this traffic class. • Enter the amount of bandwidth, in kilobits per second (kbps).
Step 6	Repeat Steps Configuring and Applying Bandwidth-Remaining Ratios to Subinterfaces, page 7 and Configuring and Applying Bandwidth-Remaining Ratios to Subinterfaces, page 7 to configure additional traffic classes, if needed.	
Step 7	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 8	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 9	**policy-map** *parent-policy-name* **Example:** `Router(config)# policy-map Parent`	Creates or modifies a parent policy map and enters policy-map configuration mode. • Enter the name of the parent policy map.

Step 10	**class class-default**
	Example:
	`Router(config-pmap)# class class-default`
		Configures the class-default class and enters policy-map class configuration mode.
		Note The router interprets any features that are configured under the class-default class as aggregate features on the subinterface.

	Command or Action	Purpose
Step 11	**bandwidth remaining ratio** *ratio* **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10`	Specifies the bandwidth-remaining ratio for the subinterface. • Enter the ratio. The ratio is the value used to determine the amount of unused bandwidth to allocate to each queue on the subinterface during periods of congestion. The scheduler allocates the excess bandwidth relative to other subinterfaces. Valid values are 1 to 1000. The default value is 1.
Step 12	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] **Example:** `Router(config-pmap-c)# shape average 100000000`	(Optional) Shapes the average or peak rate to the rate that you specify. • Enter either the **average** or **peak** keyword along with the CIR and any optional arguments. Note the following: ◦ average--Specifies average-rate shaping. ◦ peak--Specifies peak-rate shaping. ◦ cir--Specifies the committed information rate (CIR), in bits per second (bps). ◦ (Optional) bc--Specifies the committed burst size, in bits. ◦ (Optional) be--Specifies the excess burst size, in bits.
Step 13	**service-policy** *child-policy-name* **Example:** `Router(config-pmap-c)# service-policy Child`	Applies the child policy map that you specify to the traffic class. • Enter the name of the previously configured child policy map. The router applies the QoS actions (features) specified in the child policy map to the traffic class. **Note** The **service-policy** command typically requires that you specify the direction of the traffic using the input or output keywords. However, when applying a child policy to a parent policy, do not specify a traffic direction.
Step 14	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 15	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.

	Command or Action	Purpose
Step 16	**interface** *type slot* / *module* / *port* **.** *subinterface* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface GigabitEthernet 1/0/0.1`	Creates or modifies the interface that you specify and enters subinterface configuration mode. • Enter the interface type. Note the following: ◦ type--Specifies the interface type (for example, Gigabit Ethernet). ◦ slot/module/port.subinterface--Specifies the number of the subinterface that identifies the subinterface (for example, 1/0/0.1). ◦ (Optional) point-to-point--Indicates that the subinterface is a point-to-point subinterface. ◦ (Optional) multipoint--Indicates that the subinterface is a point-to-multipoint subinterface.
Step 17	**service-policy output** *parent-policy-name* **Example:** `Router(config-subif)# service-policy output Parent`	Applies the parent policy map to the subinterface. • Enter the **output** keyword and the name of the parent policy map. **Note** The router shapes the subinterface traffic to the shaping rate specified in the parent class-default class and applies the QoS actions (features) specified in the child policy map. **Note** During periods of congestion, the router uses the bandwidth-remaining ratio specified in the parent policy map to allocate unused bandwidth on this subinterface relative to other subinterfaces.

Step 18	**end**
	Example:
	`Router(config-subif)# end`
		Returns to privileged EXEC mode.

Configuring and Applying Bandwidth-Remaining Ratios to Class Queues

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *child-policy-name*
4. **class** *class-map-name*
5. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
6. **bandwidth remaining ratio** *ratio*
7. Repeat Steps Configuring and Applying Bandwidth-Remaining Ratios to Class Queues, page 12, Configuring and Applying Bandwidth-Remaining Ratios to Class Queues, page 12, and Configuring and Applying Bandwidth-Remaining Ratios to Class Queues, page 12 for each class queue that you want to define, specifying the bandwidth-remaining ratio as applicable.
8. **exit**
9. **exit**
10. **policy-map** *parent-policy-name*
11. **class class-default**
12. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
13. **bandwidth remaining ratio** *ratio*
14. **service-policy** *child-policy-name*
15. **exit**
16. **exit**
17. **interface** *type slot* / *module* / *port* **.** *subinterface* [**point-to-point** | **multipoint**]
18. **service-policy output** *parent-policy-name*
19. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map** *child-policy-name* **Example:** `Router(config)# policy-map Child`	Creates or modifies a child policy map and enters policy-map configuration mode. • Enter the name of the child policy map.

Step 4	**class** *class-map-name*
	Example:
	`Router(config-pmap)# class precedence_0`
		Configures the class map and enters policy-map class configuration mode.

Step 5	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] **Example:** `Router(config-pmap-c)# shape average 100000000`	(Optional) Shapes the average or peak rate to the rate that you specify. • Enter either the **average** or **peak** keyword along with the CIR and any optional arguments. Note the following: ◦ average--Specifies average-rate shaping. ◦ peak--Specifies peak-rate shaping. ◦ cir--Specifies the committed information rate (CIR), in bits per second (bps). ◦ (Optional) bc--Specifies the committed burst size, in bits. ◦ (Optional) be--Specifies the excess burst size, in bits.
Step 6	**bandwidth remaining ratio** *ratio* **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10`	Specifies the bandwidth-remaining ratio for the traffic class. • Enter the bandwidth-remaining ratio. The ratio is the value used to determine the amount of unused bandwidth to allocate to each queue on the subinterface during periods of congestion. The queueing mechanism or scheduler allocates the excess bandwidth relative to other subinterfaces. Valid values are 1 to 1000. The default value is 1. **Note** In a hierarchical policy map structure, the **bandwidth remaining ratio***ratio* command must be used for at least one class. Using it in other classes is optional. When this command is not explicitly enabled in the other classes, the queueing mechanism uses 1 as the default.
Step 7	Repeat Steps Configuring and Applying Bandwidth-Remaining Ratios to Class Queues, page 12, Configuring and Applying Bandwidth-Remaining Ratios to Class Queues, page 12, and Configuring and Applying Bandwidth-Remaining Ratios to Class Queues, page 12 for each class queue that you want to define, specifying the bandwidth-remaining ratio as applicable.	

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 9	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 10	**policy-map** *parent-policy-name* **Example:** `Router(config)# policy-map Parent`	Creates or modifies a parent policy map and enters policy-map configuration mode. • Enter the name of the parent policy map.

Step 11	**class class-default**
	Example:
	`Router(config-pmap)# class class-default`
		Configures the class-default class and enters policy-map class configuration mode.
		Note The router interprets any features that are configured under the class-default class as aggregate features on the subinterface.

Step 12	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] **Example:** `Router(config-pmap-c)# shape average 100000000`	(Optional) Shapes the average or peak rate to the rate that you specify. • Enter either the **average** or **peak** keyword along with the CIR and any optional arguments. Note the following: ◦ average--Specifies average-rate shaping. ◦ peak--Specifies peak-rate shaping. ◦ cir--Specifies the committed information rate (CIR), in bits per second (bps). ◦ (Optional) bc--Specifies the committed burst size, in bits. ◦ (Optional) be--Specifies the excess burst size, in bits.

	Command or Action	Purpose
Step 13	**bandwidth remaining ratio** *ratio* **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10`	(Optional for class-default or other classes in a hierarchical policy map structure) Specifies the bandwidth-remaining ratio for the subinterface. • Enter the bandwidth-remaining ratio. The ratio is the value used to determine the amount of unused bandwidth to allocate to each queue on the subinterface during periods of congestion. The queueing mechanism or scheduler allocates the excess bandwidth relative to other subinterfaces. Valid values are 1 to 1000. The default value is 1. **Note** In a hierarchical policy map structure, the **bandwidth remaining ratio***ratio* command must be used for at least one class. Using it in other classes is optional. When this command is not explicitly enabled in the other classes, the queueing mechanism uses 1 as the default.
Step 14	**service-policy** *child-policy-name* **Example:** `Router(config-pmap-c)# service-policy Child`	Applies the child policy map that you specify to the traffic class. • Enter the name of the child policy map. The router applies the QoS actions (features) specified in the child policy map to the traffic class. **Note** The **service-policy**command typically requires that you specify the direction of the traffic using the input or output keywords. However, when applying a child policy map to a parent policy map, do not specify traffic direction.
Step 15	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 16	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 17	**interface** *type slot* **/** *module* **/** *port* **.** *subinterface* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface GigabitEthernet 1/0/0.1`	Creates or modifies the interface that you specify and enters subinterface configuration mode. • Enter the interface type. Note the following: ◦ type--Specifies the interface type (for example, Gigabit Ethernet). ◦ slot/module/port.subinterface--Specifies the number of the subinterface that identifies the subinterface (for example, 1/0/0.1). ◦ (Optional) point-to-point--Indicates that the subinterface is a point-to-point subinterface. ◦ (Optional) multipoint--Indicates that the subinterface is a point-to-multipoint subinterface.

	Command or Action	Purpose
Step 18	**service-policy output** *parent-policy-name* **Example:** `Router(config-subif)# service-policy output Parent`	Attaches the parent policy map to the subinterface. • Enter the **output**keyword and the name of the parent policy map. **Note** When congestion occurs, the class queues receive bandwidth according to the specified class-level bandwidth-remaining ratios.

Step 19	**end**
	Example:
	`Router(config-subif)# end`
		Returns to privileged EXEC mode.

Configuration Examples for Distribution of Remaining Bandwidth Using Ratio

Example Configuring Bandwidth-Remaining Ratios on Ethernet Subinterfaces

The following example shows how to configure bandwidth-remaining ratios on an Ethernet subinterface using a hierarchical policy. In the example, Gigabit Ethernet subinterface 1/0/0.1 is shaped to 100 Mbps. During congestion, the router uses the bandwidth-remaining ratio of 10 to determine the amount of excess bandwidth (unused by priority traffic) to allocate to the nonpriority traffic on subinterface 1/0/0.1, relative to the other subinterface-level and class-level queues on the interface.

```
policy-map Child
 class precedence_0
  bandwidth 10000
 class precedence_1
  shape average 100000
  bandwidth 100
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  shape average 100000000
  service-policy Child
interface GigabitEthernet1/0/0.1
 encapsulation dot1Q 100
 ip address 10.1.0.1 255.255.255.0
 service-policy output Parent
```

Example Verifying Bandwidth-Remaining Ratios on Class Queues

In the following sample configuration, vlan10_policy is applied on the Gigabit Ethernet subinterface 1/0/0.10 and vlan20_policy is applied on the Gigabit Ethernet subinterface 1/0/0.20. During congestion on the interface, subinterface Gigabit Ethernet 1/0/0.20 has 10 times more available bandwidth than subinterface Gigabit Ethernet 1/0/0.10 because the bandwidth-remaining ratio for subinterface Gigabit Ethernet 1/0/0.20 is 10 times more than the bandwidth-remaining ratio for subinterface 1/0/0.10: 100 on subinterface 1/0/0.20 and 10 on subinterface 1/0/0.10.

When congestion occurs within a subinterface level, the class queues receive bandwidth according to the class-level bandwidth-remaining ratios. In the example, the bandwidth for classes precedence_0, precedence_1, and precedence_2 is allocated based on the bandwidth-remaining ratios of the classes: 20, 40, and 60, respectively.

Router# **show policy-map**

```
Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20 <---- Class-level ratio
    Class precedence_1
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 40 <---- Class-level ratio
    Class precedence_2
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 60 <---- Class-level ratio
Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10 <---- Subinterface-level ratio
      service-policy child-policy
Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 100 <---- Subinterface-level ratio
      service-policy child-policy
interface GigabitEthernet1/0/0.10
 encapsulation dot1Q 10
 snmp trap link-status
 service-policy output vlan10_policy
interface GigabitEthernet1/0/0.20
 encapsulation dot1Q 20
 snmp trap link-status
 service-policy output vlan20_policy
```

Example Verifying Bandwidth Remaining Ratios

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured on class-level queues in the policy maps named vlan10_policy and child-policy, which are attached to Gigabit Ethernet subinterface 1/0/0.10.

```
Router# show policy-map interface GigabitEthernet 1/0/0.10
GigabitEthernet1/0/0.10
  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 10
      Service-policy : child-policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured on class-level queues in the policy maps named vlan20_policy and child-policy, which are attached to Gigabit Ethernet subinterface 1/0/0.20.

```
Router# show policy-map interface GigabitEthernet 1/0/0.20
GigabitEthernet1/0/0.20
  Service-policy output: vlan20_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 100
      Service-policy : child-policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

The following sample output from the show policy-map command indicates that a bandwidth-remaining ratio of 10 is configured on the parent class-default class of the policy map named vlan10_policy.

```
Router# show policy-map vlan10_policy
  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10
      service-policy child-policy
```

The following sample output from the show policy-map command indicates that a bandwidth-remaining ratio of 100 is configured on the parent class-default class of the policy map named vlan20_policy.

```
Router# show policy-map vlan20_policy
  Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 100
      service-policy child-policy
```

The following sample output from the show policy-map command indicates that bandwidth-remaining ratios of 20, 40, and 60 are configured on the class queues precedence_0, precedence_1, and precedence_2, respectively.

```
Router# show policy-map child-policy
  Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20
```

```
Class precedence_1
  Average Rate Traffic Shaping
  cir 500000 (bps)
  bandwidth remaining ratio 40
Class precedence_2
  Average Rate Traffic Shaping
  cir 500000 (bps)
  bandwidth remaining ratio 60
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Congestion avoidance	"Congestion Avoidance Overview" module
Class maps, policy maps, hierarchical policy maps, Modular Quality of Service Command-Line Interface (CLI) (MQC)	"Applying QoS Features Using the MQC" module
Traffic shaping, traffic policing	"Policing and Shaping Overview" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Distribution of Remaining Bandwidth Using Ratio

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Distribution of Remaining Bandwidth Using Ratio

Feature Name	Releases	Feature Information
MQC--Distribution of Remaining Bandwidth Using Ratio	Cisco IOS XE Release 2.1	The Distribution of Remaining Bandwidth Using Ratio feature allows service providers to configure a bandwidth-remaining ratio on subinterfaces and class queues. This ratio specifies the relative weight of a subinterface or queue with respect to other subinterfaces or queues. During congestion, the router uses this bandwidth-remaining ratio to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class of nonpriority traffic. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **bandwidth remaining ratio**, **show policy-map**, **show policy-map interface**.

QoS Percentage-Based Shaping

The QoS: Percentage-Based Shaping feature allows you to configure traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About QoS Percentage-Based Shaping

Benefits for QoS Percentage-Based Shaping

This feature provides the ability to configure traffic shaping on the basis of a percentage of bandwidth available on an interface, and it allows you to specify burst sizes in milliseconds. Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. That is, you do not have to recalculate the bandwidth for each interface or configure a different policy map for each type of interface.

Class and Policy Maps for QoS Percentage-Based Shaping

To configure the QoS: Percentage-Based Shaping feature, you must define a traffic class, configure a policy map, and then attach that policy map to the appropriate interface.

In the MQC, the **class-map** command is used to define a traffic class (which is then associated with a traffic policy). The purpose of a traffic class is to classify traffic.

The MQC consists of the following three processes:

- Defining a traffic class with the **class-map** command.
- Creating a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).
- Attaching the traffic policy to the interface with the **service-policy** command.

A traffic class contains three major elements: a name, a series of match commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands (that is, match-all or match-any). The traffic class is named in the **class-map** command line; for example, if you enter the **class-map cisco** command while configuring the traffic class in the CLI, the traffic class would be named "cisco".

The **match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

Traffic Regulation Mechanisms and Bandwidth Percentages

Cisco IOS XE quality of service (QoS) offers two kinds of traffic regulation mechanisms--traffic policing and traffic shaping. A traffic policer typically drops traffic that violates a specific rate. A traffic shaper typically delays excess traffic using a buffer to hold packets and shapes the flow when the data rate to a queue is higher than expected.

Traffic shaping and traffic policing can work in tandem and can be configured in a class map. Class maps organize data packets into specific categories ("classes") that can, in turn, receive a user-defined QoS treatment when used in policy maps (sometimes referred to as "service policies").

Before this feature, traffic policing and traffic shaping were configured on the basis of a user-specified amount of bandwidth available on the interface. Policy maps were then configured on the basis of that specific amount of bandwidth, meaning that separate policy maps were required for each interface.

This feature provides the ability to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. Configuring traffic policing and traffic shaping in this manner enables customers to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Configuring traffic policing and shaping on the basis of a percentage of bandwidth is accomplished by using the **police** (percent) and **shape** (percent) commands.

Burst Size Specified in Milliseconds Option

The purpose of the burst parameters (bc and be) is to specify the amount of traffic to anticipate under normal operating conditions before traffic is dropped or delayed. Setting sufficiently high burst values helps to ensure good throughput.

This feature allows you the option of specifying the committed (conform) burst (bc) size and the excess (peak) burst (be) as milliseconds (ms) of the class bandwidth when you configure traffic shaping. The number of milliseconds is used to calculate the number of bytes to be used by the QoS: Percentage-Based Shaping feature.

Specifying these burst sizes in milliseconds is accomplished by using the **bc** and **be** keywords (and their associated arguments) of the **shape** (percent) command.

How to Configure QoS Percentage-Based Shaping

- Configuring a Class and Policy Map, page 25
- Attaching the Policy Map to an Interface, page 26
- Verifying the QoS Percentage-Based Shaping Configuration, page 28

Configuring a Class and Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name*| **class-default**}
5. **shape** {**average** | **peak**} **percent** *percentage* [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map to be created. Enters policy-map configuration mode. • Enter the policy map name.

Step 4	**class** {*class-name*| **class-default**}
	Example:
	`Router(config-pmap)# class class1`
		Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.
		• Enter the class name or specify the default class (class-default).

Step 5	**shape** {**average** | **peak**} **percent** *percentage* [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**] **Example:** `Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms`	Configures either average or peak rate traffic shaping on the basis of the specified bandwidth percentage and the optional burst sizes. • Enter the bandwidth percentage and optional burst sizes.

Step 6	**end**
	Example:
	`Router(config-pmap-c)# end`
		Exits policy-map class configuration mode.

Attaching the Policy Map to an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**interface** *type number*
	Example:
	`Router(config)#`
	`interface serial4/0/0`
		Configures an interface (or subinterface) type and enters interface configuration mode.
		- Enter the interface type number.
		Note Depending on the needs of your network, you may need to attach the policy map to a subinterface, an ATM PVC, a Frame Relay DLCI, or other type of interface.

Step 4	**pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	(Optional) Creates or assigns a name to an ATM PVC and specifies the encapsulation type on an ATM PVC. Enters ATM VC configuration mode. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, skip this step and proceed with Attaching the Policy Map to an Interface, page 26.

Step 5	**service-policy** {**input**| **output**} *policy-map-name*
	Example:
	`Router(config-if)#`
	`service-policy input policy1`
	Example:
		Specifies the name of the policy map to be attached to the input or output direction of the interface.
		Note Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
		Note Traffic shaping is supported on service policies attached to output interfaces or output VCs only.
		- Enter the policy map name.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Exits interface configuration mode.

Verifying the QoS Percentage-Based Shaping Configuration

SUMMARY STEPS

1. **enable**
2. **show class-map** [*class-map-name*]
3. **show policy-map interface** *interface-name*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** [*class-map-name*] **Example:** `Router# show class-map class1`	Displays all information about a class map, including the match criterion. • Enter class map name.

Step 3	**show policy-map interface** *interface-name*
	Example:
	`Router#`
	`show policy-map interface serial4/0/0`
		Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		• Enter the interface type and number.

Step 4	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

- Troubleshooting Tips, page 29

Troubleshooting Tips

The commands in the Verifying the QoS Percentage-Based Shaping Configuration, page 28 section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If, after using the **show** commands listed above, you find that the configuration is not correct or the feature is not functioning as expected, perform these operations:

If the configuration is not the one you intended, complete the following procedures:

1. Use the **show running-config** command and analyze the output of the command.
2. If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
3. Attach the policy map to the interface again.

If the packets are not being matched correctly (for example, the packet counters are not incrementing correctly), complete the following procedures:

1. Run the **show policy-map**command and analyze the output of the command.
2. Run the **show running-config** command and analyze the output of the command.
3. Use the **show policy-map interface** command and analyze the output of the command. Check the the following findings:

   a. If a policy map applies queueing, and the packets are matching the correct class, but you see unexpected results, compare the number of the packets in the queue with the number of the packets matched.
   b. If the interface is congested, and only a small number of the packets are being matched, check the tuning of the transmission (tx) ring, and evaluate whether the queueing is happening on the tx ring. To do this, use the **show controllers** command, and look at the value of the tx count in the output of the command.

Configuration Examples for QoS Percentage-Based Shaping

- Example Specifying Traffic Shaping on the Basis of a Bandwidth Percentage, page 29
- Example Verifying the QoS Percentage-Based Shaping Configuration, page 30

Example Specifying Traffic Shaping on the Basis of a Bandwidth Percentage

The following example configures traffic shaping using an average shaping rate on the basis of a percentage of bandwidth. In this example, 25 percent of the bandwidth has been specified. Additionally, an optional be value and bc value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1


Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms


Router(config-pmap-c)# end
```

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)#

interface serial4/0/0
Router(config-if)#

service-policy input policy1
Router(config-if)# end
```

Example Verifying the QoS Percentage-Based Shaping Configuration

This section contains sample output from the **show policy-map**command and the **show policy-map interface**command. The output from these commands can be used to verify and monitor the configuration on your network.

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called "policy3." In policy 3, average rate traffic shaping on the basis of an committed information rate (CIR) of 30 percent has been configured, and the bc and be have been specified in milliseconds.

```
Router# show policy-map
  Policy Map policy3
    Class class-default
      Average Rate Traffic Shaping
      cir 30% bc 10 (msec) be 10 (msec)
```

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which average rate traffic shaping has been enabled.

```
Router# show policy-map interface serial2/0/0
 Serial2/0/0
  Service-policy output: policy3 (1032)
    Class-map: class-default (match-any) (1033/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1034)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 0/0
      shape (average) cir 614400 bc 6144 be 6144
      target shape rate 614400
```

In this example, the CIR is displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, bc, and be are calculated on the basis of the formulas described below.

Formula for Calculating the CIR

When calculating the CIR, the following formula is used:

CIR percentage specified (as shown in the output of the **show policy-map**command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

On the serial 2/0 interface, the bandwidth (BW) is 2048 kbps. To see the bandwidth of the interface, use the **show interfaces** command. A sample is shown below:

```
Router # show interfaces serial2/0/0
Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

Therefore, the following values are used in the formula:

30% * 2048 kbps = 614400 bps

Formula for Calculating the Committed Burst (bc) and the Excess Burst (be)

When calculating both the bc and the be, the following formula is used:

The bc (or be) in milliseconds (as shown in the **show policy-map** command) * the CIR in kilobytes (as shown in the **show policy-map** command) / 1000 = total number of bits

Therefore, the following values are used in the formula:

10 ms * 614400 bps = 6144 bits

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Modular QoS Command-Line Interface (CLI) (MQC) information about attaching policy maps to interfaces	"Applying QoS Features Using the MQC" module
Traffic shaping concepts and overview	"Policing and Shaping Overview" module
Traffic policing	"Traffic Policing" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2697	*A Single Rate Three Color Marker*
RFC 2698	*A Two Rate Three Color Marker*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for QoS Percentage-Based Shaping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for QoS: Percentage-Based Shaping

Feature Name	Releases	Feature Information
QoS: Percentage-Based Shaping	Cisco IOS XE Release 2.1	The QoS: Percentage-Based Shaping feature allows you to configure traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed (conform) burst (bc) size and the excess (peak) burst (be) size (used for configuring traffic shaping) in milliseconds (ms). Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. This feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **shape (percent)**, **show policy-map**, **show policy-map interface**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Ethernet Overhead Accounting

The Ethernet Overhead Accounting feature enables the router to account for downstream Ethernet frame headers when applying shaping to packets.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Ethernet Overhead Accounting

- Ethernet overhead accounting allows the automatic inclusion of downstream Ethernet frame headers in the shaped rate. However, policing is not supported for Ethernet overhead accounting
- The router supports overhead accounting only for the shape and bandwidth commands.
- If you enable overhead accounting on a child policy, then you must enable overhead accounting on the parent policy.
- In a policy map, you must either enable overhead accounting for all classes in the policy or disable overhead accounting for all classes in the policy. You cannot enable overhead accounting for some classes and disable overhead accounting for other classes in the same policy.
- When you enter the show policy-map interface command, the resulting classification byte counts and the queueing feature byte counts do not match. This mismatch occurs because the classification byte count does not consider overhead, whereas the queueing features do consider overhead.
- You can enable overhead accounting for shaping and bandwidth on top-level parent policies, middle-level child policies, and bottom-level child policies.

- If you enable overhead accounting on a parent policy, you are required to enable accounting on a child policy that is configured with the shape or bandwidth command. You are not required to enable accounting on a child policy that does not have the shape or bandwidth command configured.

Information About Ethernet Overhead Accounting

Benefits of Ethernet Overhead Accounting

The Ethernet Overhead Accounting feature enables the router to account for downstream Ethernet frame headers when applying shaping to packets. A user-defined offset specifies the number of overhead bytes that the router is to use when calculating the overhead per packet Valid offset values are from +63 bytes to -63 bytes of overhead. Before applying shaping, the router calculates teh overhead.

Ethernet interfaces and subinterfaces support overhead accounting. Using the shape or bandwidth command, you can configure accounting per VLAN and per port.

Subscriber Line Encapsulation Types

The subscriber-encap option of the shape and bandwidth commands specifies the encapsulation type at the subscriber line. The router supports the following subscriber line encapsulation types:

- snap-1483routed
- mux-1483routed
- snap-dot1q-rbe
- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-rbe
- mux-rbe

Overhead Calculation on the Router

When calculating overhead for traffic shaping, the router considers the encapsulation type used between the BRAS and the DSLAM and between the DSLAM and the CPE.

The table below describes the fields that the router uses for the various encapsulation types when calculating ATM overhead.

Table 3 Overhead Calculation

Encapsulation Type	Number of Bytes	Description
802.1Q	18	6-byte destination MAC address + 6-byte source MAC address + 2-byte protocol ID (0x8100) + 2-byte VID/CFI/PRIORITY + 2-byte length/type
802.3	14	6-byte destination MAC address + 6-byte source MAC address + 2-byte protocol ID (0x8000)
AAL5 MUX plus 1483	8	8-byte AAL5 trailer
AAL5 MUX plus PPPoA	10	8-byte AAL5 trailer + 2-byte protocol ID (0x002
AAL5 SNAP plus 1483	18	8-byte AAL5 trailer + 3-byte LLC header (0xAAAA03) + 3-byte OUI (0x0080c2) + 2-byte protocol ID (0x0007) + 2-byte PAD (0x0000)
AAL5 SNAP plus PPPoA	12	8-byte AAL5 trailer + 3-byte LLC header (0xFEFE03) + 1-byte protocol ID (0xCF)
PPPoE	6	1-byte version/type (0x11) + 1-byte code (0x00) + 2-byte session ID + 2-byte lengt
qinq	22	6-byte destination MAC address + 6-byte source MAC address + 2-byte protocol ID (0x8100) + 2-byte VID/CFI/PRIORITY + 2-byte protocol ID + 2-byte inner tag + 2-byte length or type

Overhead Accounting and Hierarchical Policies

In hierarchical policies, you can enable overhead accounting for shaping and bandwidth on top-level parent policies, middle-level child policies, and bottom-level child policies. If you enable overhead accounting on a:

- Parent class-default class, then you are not required to enable accounting on a child traffic class that does not contain the bandwidth or shape command.
- Child policy, then you must enable overhead accounting on the parent policy.

The parent and child classes must specify the same encapsulation type when enabling overhead accounting and configuring an offset using the user-defined offset [atm] command option.

The table below summarizes the configuration requirements for overhead accounting. For example, if overhead accounting is currently enabled for a parent policy, then accounting can be disabled or enabled on a child policy.

Table 4 Overhead Accounting Configuration Requirements

Policy Map or Class	Current Configuration	Configuration Requirement
Parent	Enabled	Enabled on child policy
Child	Enabled	Enabled on parent policy
Child class	Enabled	Enabled on all classes in the child policy map, except priority classes with policing
Child class (nonpriority without policing)	Disabled	Disabled on all classes in the child policy map
Child class (priority with policing)	Disabled	Disabled or enabled on all nonpriority classes in the child policy map

How to Configure Ethernet Overhead Accounting

- Configuring Ethernet Overhead Accounting in a Hierarchical Policy, page 38
- Verifying Overhead Accounting, page 41

Configuring Ethernet Overhead Accounting in a Hierarchical Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. **bandwidth** {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*} [**account** {{**qinq** | **dot1q**} {**aal5**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}]
6. exit
7. **policy-map** *policy-map-name*
8. **class** *class-default*
9. **shape** [**average**] *rate*[**account** {{**qinq** | **dot1q**} [**aal5**] {*subscriber-encap*}} | {**user-defined** *offset* [**atm**]}]
10. **service-policy** *policy-map-name*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map Business`	Creates or modifies the child policy. Enters policy-map configuration mode. • The policy-map-name argument represents the name of the child policy map.

Step 4	**class** *class-map-name*
	Example:
	`Router(config-pmap)# class video`
		Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode.
		• The class-map-name argument represents the name of a previously configured class map.

	Command or Action	Purpose
Step 5	**bandwidth** {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*} [**account** {{**qinq** | **dot1q**} {**aal5**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}] **Example:** `Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`	Enables class-based fair queueing and overhead accounting. • bandwidth-kbps--Specifies or modifies the minimum bandwidth allocated for a class belonging to a policy map. Valid values are from 8 to 2,488,320, which represents from 1 to 99 percent of the link bandwidth. • percentage--Specifies or modifies the maximum percentage of the link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • remaining percentage--Specifies or modifies the minimum percentage of unused link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • account--Enables ATM overhead accounting. • qinq--Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • dot1q--Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • aal5--Specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. • subscriber-encapsulation--Specifies the encapsulation type at the subscriber line. For more information, see the Configuring Ethernet Overhead Accounting in a Hierarchical Policy, page 38. • user-defined--Indicates that the router is to use the offset value that you specify when calculating ATM overhead. • offset--Specifies the number of bytes that the router is to use when calculating overhead. Valid values are from -63 to 63 bytes. • atm--(Optional) Applies the ATM cell tax in the ATM overhead calculation.
Step 6	exit **Example:** `router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map Test`	Creates or modifies the top-level parent policy. • policy-map-name--Specifies the name of the parent policy map.

Step 8	**class** *class-default*
	Example:
	`Router(config-pmap)# class class-default`
		Configures or modifies the parent class-default class.

	Command or Action	Purpose
Step 9	**shape** [**average**] *rate*[**account** {{**qinq** | **dot1q**} [**aal5**] {*subscriber-encap*}} | {**user-defined** *offset* [**atm**]}] **Example:** `Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1-rbe`	Shapes traffic to the indicated bit rate and enables overhead accounting. • average (Optional)--Is the committed burst (Bc) that specifies the maximum number of bits sent out in each interval. This option is only supported on the PRE3. • rate--Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that are permitted. • account--Enables ATM overhead accounting. • qinq--Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • dot1q--Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • aal5--Specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. • subscriber-encap--Specifies the encapsulation type at the subscriber line. For more information, see the Configuring Ethernet Overhead Accounting in a Hierarchical Policy, page 38. • user-defined--Indicates that the router is to use the offset value you specify when calculating ATM overhead. • offset--Specifies the number of bytes the router is to use when calculating overhead. Valid values are from -63 to +63 bytes. The router configures the offset size if you do not specify the offset option. • atm--Applies the ATM cell tax in the ATM overhead calculation. Configuring both the offset and atm options adjusts the packet size to the offset size and then adds the ATM cell tax.
Step 10	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy policy-map-name`	Applies a child policy to the parent class-default class. policy-map-name--Specifies the name of a previously configured child policy map. **Note** Do not specify the input or output keywords when applying a child policy to a parent class-default class.

Step 11	**end**
	Example:
	`Router(config-pmap-c)# end`	

Verifying Overhead Accounting

Configuration Examples for Ethernet Overhead Accounting

Example Enabling Ethernet Overhead Accounting

The following configuration example shows how to enable Ethernet overhead accounting. In the example, the configuration of the policy map named ethernet_ovrh shapes class-default traffic at a rate of 200,000 kbps and enables overhead accounting with a user-defined value of 18. The ethernet_ovrh policy is attached to Gigabit Ethernet subinterface 1/0/0.100, thereby enabling overhead accounting on the subinterface.

```
Router# configure-terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map ethernet_ovrh
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 200000 account user-defined 18
!
Router(config)# interface GigabitEthernet1/0/0.100
Router(config-subif)# service-policy output ethernet_ovrh
!
Router# show running-config | begin 1/0/0.100
interface GigabitEthernet1/0/0.100
encapsulation dot1Q 101
pppoe enable group group_pta
service-policy output ethernet_ovrh
```

Example Verifying Ethernet Overhead Accounting

The following partial sample output from the show running-config command indicates that ATM overhead accounting is enabled for shaping. The BRAS-DSLAM encapsulation is dot1q and the subscriber line encapsulation is snap-rbe based on the AAL5 service.

```
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average 10 account dot1q aal5 snap-rbe
```

Example Verifying Ethernet Overhead Accounting with User-Defined Option

The following sample output for the policy map named ethernet_ovrh indicates that Ethernet overhead accounting is enabled for shaping and that the user-defined offset is 18 bytes. The sample output from the

showpolicy-mapinterface command indicates that the ethernet_ovrh policy map is attached to the Gigabit Ethernet subinterface 1/0/0.100, enabling overhead accounting on the subinterface.

```
Router# show policy-map ethernet_ovrh
Policy Map ethernet_ovrh
Class class-default
Average Rate Traffic Shaping
cir 200000 (bps) account user-defined 18
Router# show policy-map interface GigabitEthernet1/0/0.100
GigabitEthernet1/0/0.100
Service-policy output: ethernet_ovrh
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 8 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 200000, bc 800, be 800
target shape rate 200000
Overhead Accounting Enabled
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Policing and Shaping.	"Policing and Shaping Overview" module
Class maps	"Applying QoS Features Using the MQC" module
Policy maps	"Applying QoS Features Using the MQC" module

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Ethernet Overhead Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 Feature Information for Ethernet Overhead Accounting

Feature Name	Releases	Feature Information
Ethernet Overhead Accounting	Cisco IOS XE Release 2.4	The Ethernet Overhead Accounting feature was introduced on the Cisco ASR 1000 series routers.

MQC Traffic Shaping Overhead Accounting for ATM

The MQC Traffic Shaping Overhead Accounting for ATM feature enables a broadband aggregation system (BRAS) to account for various encapsulation types when applying quality of service (QoS) functionality to packets. Typically, in Ethernet digital subscriber line (DSL) environments, the encapsulation from the router to the digital subscriber line access multiplexer (DSLAM) is Gigabit Ethernet and the encapsulation from the DSLAM to the customer premises equipment (CPE) is ATM. ATM overhead accounting enables the router to account for ATM encapsulation on the subscriber line and for the overhead added by cell segmentation. This functionality enables the service provider to prevent overruns at the subscriber line and ensures that the router executes QoS features on the actual bandwidth used by ATM packets.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Traffic Shaping Overhead Accounting for ATM

Traffic classes must be configured using the **class-map** command.

Restrictions for Traffic Shaping Overhead Accounting for ATM

- The encapsulation type used within a policy map and between the parent policy map and the child policy map (in a hierarchical policy map structure) must be consistent.
- You must attach a policy map that is configured with ATM overhead accounting to only an Ethernet interface (or an IP session on an Ethernet interface).

Information About Traffic Shaping Overhead Accounting for ATM

Benefits of Traffic Shaping Overhead Accounting for ATM

The Traffic Shaping Overhead Accounting for ATM feature enables the broadband aggregation system (BRAS) to account for various encapsulation types when applying QoS to packets. Typically, in Ethernet digital subscriber line (DSL) environments, the encapsulation from the BRAS to the DSLAM is Gigabit Ethernet and the encapsulation from the DSLAM to the CPE is ATM. ATM overhead accounting enables the BRAS to account for ATM encapsulation on the subscriber line and for the overhead added by cell segmentation. This functionality enables the service provider to prevent overruns at the subscriber line and ensures that the router executes QoS features on the actual bandwidth used by ATM subscriber traffic.

BRAS and Encapsulation Types

Broadband aggregation system (BRAS) uses the encapsulation type that is configured for the DSLAM-CPE side to calculate the ATM overhead per packet.

DSLAM-CPE encapsulation types are based on Subnetwork Access Protocol (SNAP) and multiplexer (MUX) formats of ATM adaptation layer 5 (AAL5), followed by routed bridge (RBE), x-1483, x-dot1q-rbe, IP, PPP over Ethernet (PPPoE), or PPP over ATM (PPPoA) encapsulations. Because the DSLAM treats IP and PPPoE packets as payload, the BRAS does not account for IP and PPPoE encapsulations.

On the BRAS-DSLAM side, encapsulation is IEEE 802.1Q VLAN or Q-in-Q (qinq). However, because the DSLAM removes the BRAS-DSLAM encapsulation, the BRAS does not account for 802.1Q or qinq encapsulation.

AAL5 segmentation processing adds the additional overhead of the 5-byte cell headers, the AAL5 Common Part Convergence Sublayer (CPCS) padding, and the AAL5 trailer. For more information, see the ATM Overhead Calculation, page 49.

Subscriber Line Encapsulation Types

The router supports the following subscriber line encapsulation types:

- snap-rbe
- mux-rbe
- snap-dot1q-rbe
- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-1483routed
- mux-1483routed
- snap-rbe-dot1q
- mux-rbe-dot1q

Note The encapsulation types listed above are for AAL5, qinq, and dot1q encapsulations. User-defined encapsulations with offsets based on the platform in use are also supported.

ATM Overhead Calculation

The Traffic Shaping Overhead Accounting for ATM feature prevents oversubscription of a subscriber line by accounting for the ATM encapsulation overhead at the BRAS. When calculating the ATM overhead, the Traffic Shaping Overhead Accounting for ATM feature considers the following:

- The encapsulation type used by the BRAS
- The CPCS trailer overhead
- The encapsulation type used between the DSLAM and the CPE

The offset size (a parameter used to calculate ATM overhead accounting) is calculated using the following formula:

Offset size in bytes = (CPCS trailer overhead) + (DSLAM to CPE) - (BRAS encapsulation type)

This offset size, along with the packet size and packet assembler/disassembler (PAD) byte overhead in the CPCS, is used by the router to calculate the ATM overhead accounting rate.

Note A CPCS trailer overhead of 8 bytes corresponds to AAL5. A CPCS trailer overhead of 4 bytes corresponds to AAL3, but AAL3 is not supported.

Table 6 Offset Sizes, in Bytes, Used for ATM Overhead Calculation

Encapsulation Type in Use	BRAS	CPCS Trailer Overhead	DSLAM to CPE	Offset Size
dot1q mux-1483routed	18	8	3	-7
dot1q snap-1483routed	18	8	6	-4

Encapsulation Type in Use	BRAS	CPCS Trailer Overhead	DSLAM to CPE	Offset Size
dot1q mux-rbe	18	8	14	4
dot1q snap-rbe	18	8	24	14
dot1q mux-dot1q-rbe	18	8	18	8
dot1q snap-dot1q-rbe	18	8	28	18
qot1q mux-pppoa	18 + 6	8	2	-14
qot1q snap-pppoa	18 + 6	8	4	-12
qinq mux-1483routed	22	8	3	-11
qinq snap-1483routed	22	8	6	-8
qinq mux-rbe	22	8	14	0
qinq snap-rbe	22	8	24	10
qinq mux-dot1q-rbe	22	8	18	4
qing snap-dot1q-rbe	22	8	28	14
qinq mux-pppoa	22 + 6	8	2	-18
qinq snap-pppoa	22 + 6	8	4	-16

ATM Overhead Accounting and Hierarchical Policies

In hierarchical policies, you can enable ATM overhead accounting for shaping and bandwidth on parent policies and child policies. You are not required to enable ATM overhead accounting on a traffic class that does not contain the **bandwidth** or **shape** command. If you enable ATM overhead accounting on a child policy, then you must enable ATM overhead accounting on the parent policy. The parent and child classes must specify the same encapsulation type when ATM overhead accounting is enabled.

How to Configure Traffic Shaping Overhead Accounting for ATM

- Configuring Traffic Shaping Overhead Accounting for ATM in a Hierarchical Policy, page 51
- Verifying the Configuration of Traffic Shaping Overhead Accounting for ATM, page 55

Configuring Traffic Shaping Overhead Accounting for ATM in a Hierarchical Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}}
6. **bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**|**aal3**] {*subscriber-encapsulation* | **user-defined***offset*[atm]}]
7. **shape** [**average** |**peak**] mean-*rate*[*burst-size*] [*excess-burst-size*] account {{{qinq | dot1q} {aal5 | aal3} {subscriber-encapsulation}} | {user-defined offset [atm]}}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map Business`	Creates or modifies the child policy and enters policy-map configuration mode. • Enter the policy map name. This is the name of the child policy.

Step 4	**class** *class-map-name*
	Example:
	`Router(config-pmap)# class video`
		Assigns the traffic class that you specify for the policy map and enters policy-map class configuration mode.
		• Enter the traffic class name. This is the name of the previously configured class map.

	Command or Action	Purpose

Step 5	bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}}
	Example:
	`Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`
		Enables Class-Based Weighted Fair Queueing (CBWFQ) on the basis of the keywords and arguments specified, such as the following:
		• *bandwidth-kbps* --Specifies or modifies the minimum bandwidth allocated for a class that belongs to a policy map. Valid values are from 8 to 2488320, which represents from 1 to 99 percent of the link bandwidth.
		• **percent** *percentage* --Specifies or modifies the minimum percentage of the link bandwidth allocated for a class that belongs to a policy map. Valid values are from 1 to 99.
		• **remaining percent** *percentage* --Specifies or modifies the minimum percentage of unused link bandwidth allocated for a class that belongs to a policy map. Valid values are from 1 to 99.
		• **account** --Enables ATM overhead accounting.
		• **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type.
		• **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type.
		• **aal5** --Specifies the ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services.
		• **aal3** --Specifies the ATM adaptation layer 5 that supports both connectionless and connection-oriented links.
		• *subscriber-encapsulation* --Specifies the encapsulation type at the subscriber line. For more information, see the Subscriber Line Encapsulation Types, page 49.
		• **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead.
		• *offset* --Specifies the offset size when calculating ATM overhead. Valid values are from -63 to +63 bytes.
		• **atm** --(Optional) Applies the ATM cell tax in the ATM overhead calculation.

	Command or Action	Purpose
Step 6	**bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**|**aal3**] {*subscriber-encapsulation* | **user-defined***offset*[atm]}] **Example:** `Router(config-pmap-c)# bandwidth remaining ratio 10 account dot1q aal5 snap-pppo`	(Optional) Specifies the bandwidth-remaining ratio for the subinterface along with ATM accounting parameters: - *ratio* --Specifies the bandwidth-remaining ratio for the subinterface. Valid values are 1 to 100. The default value is 1. **Note** For the Cisco 7600 series router, valid values are from 1 to 10000. The default value is 1. - **account** --Enables ATM overhead accounting. - **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. - **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. - **aal5** --Specifies the ATM adaptation layer 5 that supports connection-oriented VBR services. - **aal3** --Specifies the ATM adaptation layer 5 that supports both connectionless and connection-oriented links. - *subscriber-encapsulation* --Specifies the encapsulation type at the subscriber line. For more information, see the Subscriber Line Encapsulation Types, page 49. - **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead. - *offset* --Specifies the offset size, in bytes, when calculating ATM overhead. Valid values are from -63 to +63. - **atm** --(Optional) Applies the ATM cell tax in the ATM overhead calculation.

	Command or Action	Purpose

Step 7	**shape** [**average** |**peak**] mean-*rate*[*burst-size*] [*excess-burst-size*] account {{{qinq | dot1q} {aal5 | aal3} {subscriber-encapsulation}} | {user-defined offset [atm]}}
	Example:
	`Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1q-rbe`
		Shapes traffic to the indicated bit rate and enables ATM overhead accounting on the basis of the keywords and arguments specified, such as the following:
		• **average** --(Optional) The committed burst (Bc) that specifies the maximum number of bits sent out in each interval.
		• **peak** --(Optional) Specifies the maximum number of bits sent out in each interval (the Bc + excess burst [Be]). The Cisco 10000 router and the SIP400 (on the Cisco 7600 series router) do not support this option.
		• *mean-rate* --Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second.
		• *burst-size* --(Optional) The number of bits in a measurement interval (Bc).
		• *excess-burst-size* --(Optional) The acceptable number of bits permitted to go over the Be.
		• **account** --Enables ATM overhead accounting.
		• **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type.
		• **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type.
		• **aal5** --The ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services.
		• **aal3** --Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either aal3 or aal5.
		• *subscriber-encapsulation* --Specifies the encapsulation type at the subscriber line. For more information, see the Subscriber Line Encapsulation Types, page 49.
		• **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead.
		• *offset* --Specifies the offset size when calculating ATM overhead. Valid values are from -63 to +63 bytes.
		• **atm** --(Optional) Applies ATM cell tax in the ATM overhead calculation. Configuring both the *offset* and the **atm** options adjusts the packet size to the offset size and then adds ATM cell tax.

Step 8	**end**
	Example:
	`Router(config-pmap-c)# end`
		Exits policy-map class configuration mode and returns to privileged EXEC mode.

Verifying the Configuration of Traffic Shaping Overhead Accounting for ATM

SUMMARY STEPS

1. **enable**
2. **show policy-map** [*policy-map-name*]
3. **show policy-map session**
4. **show running-config**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map** [*policy-map-name*] **Example:** `Router# show policy-map unit-test`	(Optional) Displays the configuration of all classes for a specified policy map or of all classes for all existing policy maps. • (Optional) Enter the policy map name.
Step 3	**show policy-map session** **Example:** `Router# show policy-map session`	(Optional) Displays the QoS policy map in effect for an IPoE/PPPoE session.
Step 4	**show running-config** **Example:** `Router# show running-config`	(Optional) Displays the contents of the currently running configuration file.
Step 5	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Configuration Examples for Traffic Shaping Overhead Accounting for ATM

Example Enabling Traffic Shaping Overhead Accounting for ATM

In the following example, overhead accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber_classes and on the class-default class of the parent policy map named subscriber_line. The voip and video classes do not have accounting explicitly enabled; these classes have ATM overhead accounting implicitly enabled because the parent policy has overhead accounting enabled. Notice that the features in the parent and child policies use the same encapsulation type.

```
policy-map subscriber_classes
 class voip
  priority level 1
  police 8000
 class video
  priority level 2
  police 8000
 class gaming
  bandwidth remaining percent 80 accountaal5 snap-dot1q-rbe
 class class-default
  bandwidth remaining percent 20 accountaal5 snap-dot1q-rbe
policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 accountaal5 snap-dot1q-rbe
  shape average 512000 account aal5snap-dot1q-rbe
  service-policy subscriber_classes
```

Example Verifying Traffic Shaping Overhead Accounting for ATM

```
Router# show policy-map interface
```

```
Router# show policy-map session output

SSS session identifier 2 -
Service-policy output:  ATM_OH_POLICY
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 2500 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
       Overhead Accounting Enabled
```

The following partial output from the show running-config command indicates that ATM overhead accounting is enabled for shaping. The BRAS-DSLAM encapsulation is dot1q and the subscriber line encapsulation is snap-rbe based on the AAL5 service.

```
subscriber policy recording rules limit 64
```

```
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account dot1q aal5 snap-rbe
!
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC), hierarchical policies, policy maps	"Applying QoS Features Using the MQC" module
Policing and shaping traffic	"Policing and Shaping Overview" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MQC Traffic Shaping Overhead Accounting for ATM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7 Feature Information for MQC Traffic Shaping Overhead Accounting for ATM

Feature Name	Releases	Feature Information
MQC Traffic Shaping Overhead Accounting for ATM	Cisco IOS XE Release 2.4	The MQC Traffic Shaping Overhead Accounting for ATM feature enables a broadband aggregation system (BRAS) to account for various encapsulation types when applying QoS functionality to packets. The following commands were introduced or modified: **bandwidth (policy-map class)**, **bandwidth remaining ratio**, **shape (policy-map class)**, **show policy-map interface**, **show policy-map session**, **show running-config**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

PPP Session Queueing on ATM VCs

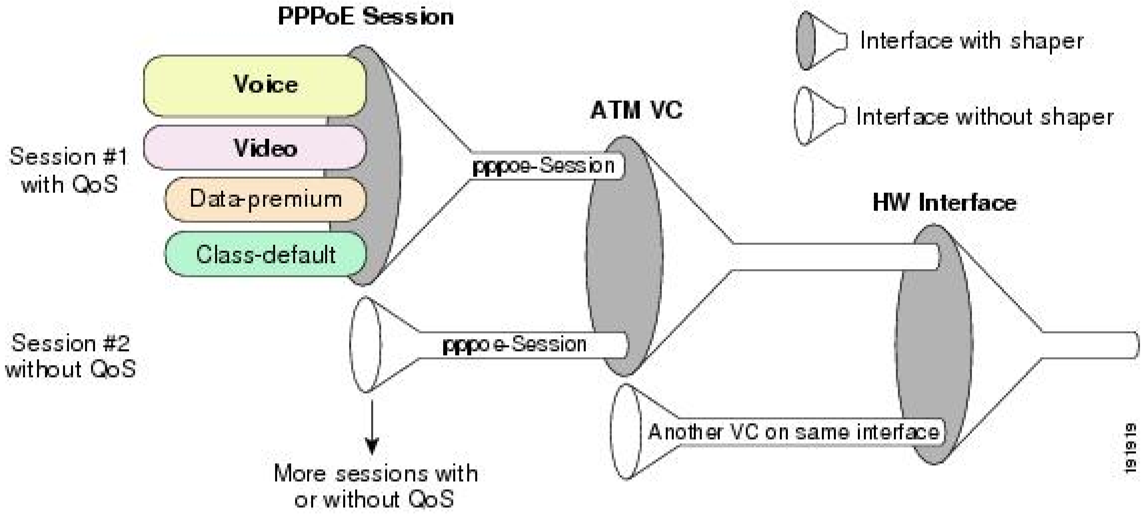
The PPP Session Queueing on ATM VCs feature enables you to shape and queue PPP over Ethernet over ATM (PPPoEoA) sessions to a user-specified rate. Multiple sessions can exist on any ATM VC and have Quality of Service (QoS) policies applied, or some of the sessions might have QoS policies. The router shapes the sum of allbandwidth used for PPPoEoA traffic on a VC so that the subscriber's connection to the Digital Subscriber Line Access Multiplexer (DSLAM) does not become congested. Queueing-related functionality provides different levels of service to the various applications that run over the PPPoEoA session.

A nested, two-level hierarchical service policy is used to configure session shaping directly on the router using the modular quality of service command-line interface (MQC). The hierarchical policy consists of the following:

- Child policy--Defines QoS actions using QoS commands such as the priority, bandwidth, and police commands.
- Parent policy--Contains only the class-default class with the shape or bandwidth remaining ratio command configured, or with both commands configured:
    - shape command--Shapes the session traffic to the specified bit rate, according to a specific algorithm.
    - bandwidth remaining ratio command--Specifies a ratio value that the router uses to determine how much unused bandwidth to allocate to the session during congestion.

Note The PPP Session Queueing on ATM VCs feature works with both PPP terminated aggregation (PTA) and L2TP access concentrator (LAC) configurations.

The figure below illustrates PPP session Queueing on ATM VCs.



Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for PPP Session Queueing on ATM VCs

- PPPoEoA sessions must be enabled.
- Create traffic classes using the class-map command and specify the match criteria used to classify traffic.
- For dynamic PPPoEoA session queueing using RADIUS, you must:
  - Enable authentication, authorization, and accounting (AAA) on the router
  - Configure the RADIUS server for dynamic QoS
  - Create the subscriber’s user profile on the RADIUS server

Restrictions for PPP Session Queueing on ATM VCs

- You cannot configure PPP session queueing on unshaped VCs--VCs without a specified peak cell rate (PCR) or sustained cell rate (SCR).
- VCs with session queueing polices cannot be part of a shaped virtual path (VP).
- If the same ATM category (for example, shaped unspecified bit rate (UBR)) contains both high and low bandwidth VCs, the SAR mechanism can cause low throughput for high bandwidth VCs. The workaround is to use different ATM classes for low and high bandwidth VCs. For example, configure low bandwidth VCs as shaped UBR and high bandwidth VCs as variable bit rate-nonreal-time (VBR-nrt) or constant bit rate (CBR).
- The CLASS-BASED QOS MIB does not include statistics for service policies applied to sessions.
- RADIUS accounting does not include queueing statistics.

Information About PPP Session Queueing on ATM VCs

Dynamically Applying QoS Policies to PPP Sessions on ATM VCs

The router allows you to dynamically apply QoS policy maps to PPPoEoA sessions using RADIUS. Although the actual configuration of the QoS policies occurs on the router, you can configure the following attribute-value (AV) pairs on RADIUS to specify the name of the policy map to dynamically apply to the session:

```
"ip:sub-qos-policy-in=<name of the QoS policy in ingress direction>"
"ip:sub-qos-policy-out=<name of egress policy>"
```

You define the AV pairs in one of the following RADIUS profiles:

- User profile--The user profile on the RADIUS server contains an entry that identifies the policy map name applicable to the user. The policy map name is the service that RADIUS downloads to the router after a session is authorized.
- Service profile--The service profile on the RADIUS server specifies a session identifier and an AV pair. The session identifier might be, for example, the IP address of the session. The AV pair defines the service (policy map name) to which the user belongs.

After receiving a service-logon request from the policy server, RADIUS sends a change of authorization (CoA) request to the router to activate the service for the subscriber, who is already logged in. If the authorization succeeds, the router downloads the name of the policy map from RADIUS using the ip:sub-qos-policy-in[out]= AV-pair and applies the QoS policy to the PPPoEoA session. Because the service policy contains queueing-related actions, the router sets up the appropriate class queues.

Note Although the router also supports the RADIUS vendor specific attribute (VSA) 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the ip:sub-qos-policy-in[out]= AV pairs for QoS policy definitions.

PPP Session Queueing Inheritance

PPP Sessions either inherit queues from their parent interface or they have their own queues. Each PPPoEoA session for which session queueing is configured has its own set of queues.

The table below describes the queues to which the router directs session traffic.

Table 8 PPP Session Queue Inheritance

Queueing Policy	Queue Used for Session Traffic
No policy	VC default queue
Applied to the VC	VC queues
Applied to the session	Session queues

Interfaces Supporting PPP Session Queueing

The router supports PPP session queueing on shaped ATM VCs for outbound traffic only.

The router does not support PPP session queueing on inbound ATM interfaces.

Mixed Configurations and Queueing

A mixed configuration is one in which all sessions do not have QoS applied to them. On some VCs, the queueing policy is applied at the VC level, and on other VCs the queueing policies are applied on the sessions. Some sessions have no policy applied at all. As a result, the router uses the hierarchical queueing framework (HQF) to direct traffic in the following ways:

- If no queueing policy is applied at the VC or session level, the router sends all traffic on the VC to the default queue, including traffic from sessions on the VC that have a policing-only policy applied or no policy applied.
- If a queueing policy is applied at the VC level, but not at the session level, the router sends traffic to the queues associated with the queueing policy on the VC.
- If queueing policies are applied to some sessions on a VC but not to other sessions, the router sends the traffic with a policing-only policy or with no policy applied to the VC's default queue. The router sends traffic with queueing policies to the queues associated with the queueing policy applied to the session.

Bandwidth Mode and ATM Port Oversubscription

An ATM port can operate in reserved bandwidth mode or shared bandwidth mode.

When a port is not oversubscribed (the sum of the bandwidths of all VCs on the port is less than the port bandwidth), the port operates in reserved bandwidth mode--a specific amount of bandwidth is reserved for each VC on the port. If a VC does not use all of its allocated bandwidth, the unused bandwidth is not shared among the VCs on the port.

When the ATM port is oversubscribed (the sum of the bandwidths of all VCs on the port is greater than the port bandwidth), the port operates in shared bandwidth mode. In this mode, any unused bandwidth is available for reuse by the other VCs on the port, up to the VC's respective shape rate--traffic on a VC cannot exceed the shape rate of that VC.

Oversubscription at the Session Level

Oversubscription at the session level occurs after session traffic shaping and when the aggregate session traffic exceeds the subinterface shape rate. After all priority traffic is accounted for, the router distributes the remaining bandwidth on the VC to the sessions according to the value specified in the bandwidth remaining ratio command configured in the parent policy of the policy applied to the sessions. If the bandwidth remaining ratio command is not specified in the parent policy, the router uses a default ratio of 1.

How to Configure PPP Session Queueing on ATM VCs

- Configuring PPP Session Queueing Using a Virtual Template, page 65
- Associating the Hierarchical Policy Map with a Virtual Template, page 69
- Applying the Virtual Template to an ATM Subinterface, page 70
- Configuring PPP Session Queueing Using Radius, page 73
- Verifying PPP Session Queueing on ATM VCs, page 74

Configuring PPP Session Queueing Using a Virtual Template

A virtual templat e is a logical interface whose configuration can specify generic configuration information for a specific purpose, user-specific configuration information, and router-dependent information. You configure a virtual template on an interface and apply QoS policy maps to the virtual template. The virtual template inherits the QoS features specified in the policy map. When the router establishes sessions on an interface, the router applies the QoS features specified in the virtual template configuration to the virtual access interfaces (VAIs) created for the sessions, including the QoS features specified in the policy map attached to the virtual template.

A broadband aggregation group (bba-group) configured on an ATM interface points to the virtual template the router uses to apply QoS policies to sessions. When a session arrives on an ATM interface, the router creates a virtual access interface (VAI) for the session and applies the policies associated with the virtual template to the sessions.

To configure PPPoEoA session queueing using a virtual template, perform the following configuration tasks:

- Configuring an Hierarchical QoS Policy, page 65

Configuring an Hierarchical QoS Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. priority level level
6. **police** *bps* [*burst-normal burst-max*] [**conform-action** *action]* [**exceed-action** *action]* **violate-action** *action*
7. set cos value
8. bandwidth remaining ratio
9. exit
10. **policy-map** *policy-map-name*
11. **class** *class-default*
12. bandwidth remaining ratio
13. **shape** [**average**] *mean-rate*[*burst-size*] [*excess-burst-size*]
14. **service-policy** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy-map-name`	Creates or modifies the child policy. Enters policy-map configuration mode. policy-map-name is the name of the child policy map.

	Command or Action	Purpose

Step 4	**class** *class-map-name*
	Example:
	`Router(config-pmap)# class class-map-name`
		Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode.
		class-map-name is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.
		Repeat Steps 2 through 6 for each traffic class you want to include in the child policy map.

Step 5	priority level level **Example:** `Router(config-pmap-c)# priority level level`	(Optional) Defines multiple levels of a strict priority service model. When you enable a traffic class with a specific level of priority service, the implication is a single priority queue associated with all traffic enabled with the specified level of priority service. level is a number that indicates a specific priority level. Valid values are from 1 (high priority) to 4 (low priority). Default: 1
Step 6	**police** *bps* [*burst-normal burst-max*] [**conform-action** *action]* [**exceed-action** *action]* **violate-action** *action* **Example:** `Router(config-pmap-c)# police bps [burst-normal] [burst-max] [conform-action action] [exceed-action action] [violate-action action]`	(Optional) Configures traffic policing. bps is the average rate in bits per second. Valid values are 8000 to 200000000. (Optional) burst-normal is the normal burst size in bytes. Valid values are 1000 to 51200000. The default normal burst size is 1500 bytes. (Optional) burst-max is the excess burst size in bytes. Valid values are 1000 to 51200000. (Optional) conform-action action indicates the action to take on packets that conform to the rate limit. (Optional) exceed-action action indicates the action to take on packets that exceed the rate limit. (Optional) violate-action action indicates the action to take on packets that violate the normal and maximum burst sizes.
Step 7	set cos value **Example:** `Router(config-pmap-c)# set cos value`	(Optional) Sets the Layer 2 class of service (CoS) value of an outgoing packet. value is a specific IEEE 802.1Q CoS value from 0 to 7.
Step 8	bandwidth remaining ratio **Example:** `Router(config-pmap-c)# bandwidth remaining ratio`	(Optional) Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non-priority queues. ratio specifies the relative weight of this subinterface or queue with respect to other subinterfaces or queues. Valid values are from 1 to 1000.

	Command or Action	Purpose
Step 9	exit **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 10	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)#` **policy-map** *policy-map-name*	Creates or modifies the parent policy. policy-map-name is the name of the parent policy map.
Step 11	**class** *class-default* **Example:** `Router(config-pmap)#` **class** *class-default*	Configures or modifies the parent class-default class. You can configure only the class-default class in a parent policy. Do not configure any other traffic class.
Step 12	bandwidth remaining ratio **Example:** `Router(config-pmap-c)# bandwidth remaining ratio`	(Optional) Specifies a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to non-priority queues. ratio specifies the relative weight of this subinterface or queue with respect to other subinterfaces or queues. Valid values are from 1 to 1000.
Step 13	**shape** [**average**] *mean-rate*[*burst-size*] [*excess-burst-size*] **Example:** **Router(config-pmap-c)# shape** `[`**average**`]` *mean-rate* `[`*burst-size*`]` `[`*excess-burst-size*`]`	Shapes traffic to the indicated bit rate and enables ATM overhead accounting. (Optional) average is the committed burst (Bc) that specifies the maximum number of bits sent out in each interval. This option is only supported on the PRE3. mean-rate is also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that are permitted. (Optional) burst-size is the number of bits in a measurement interval (Bc). (Optional) excess-burst-size is the acceptable number of bits permitted to go over the Be.
Step 14	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)#` **service-policy** *policy-map-name*	Applies the child policy to the parent class-default class. policy-map-name is the name of the child policy map configured in step 1.

Example

The following example shows how to configure a hierarchical QoS policy. In the example, the child-policy configures QoS features for two traffic classes: Premium and Silver. Premium traffic has priority and is policed at 40 percent. The router sets the IP precedence of Premium traffic to precedence level 3. Silver traffic is policed at 80000 bps and IP precedence level 3 is set. The child-policy is applied to the Parent policy class-default class, which shapes traffic to 200,000 Kbps.

```
Router(config)# policy-map child-policy
Router(config-pmap)# class Premium
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# set ip precedence 3
Router(config-pmap-c)# class Silver
Router(config-pmap-c)# police 80000 10000 conform-action transmit exceed-action drop
Router(config-pmap-c)# set ip precedence 5
Router(config-pmap-c)# exit
Router(config-pmap)# policy-map Parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 200000
Router(config-pmap-c)# service-policy output child-policy
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
```

Associating the Hierarchical Policy Map with a Virtual Template

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template template-** *number*
4. **service-policy {input | output} policy-map-name**
5. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface virtual-template template-** *number* **Example:** `Router(config)# interface virtual-template template-number`	Creates a virtual template and enters interface configuration mode. template-number is the number you assign to the virtual template interface to identify it. Valid values are from 1 to 200. You can configure up to 200 virtual template interfaces on the router.
Step 4	**service-policy {input | output} policy-map-name** **Example:** `Router(config-if)# service-policy {input | output} policy-map-name`	Attaches the policy map you specify to the virtual template interface in the inbound or outbound direction that you specify. input specifies to apply the policy map to inbound traffic. output specifies to apply the policy map to outbound traffic. policy-map-name is the name of a previously configured policy map.
Step 5	exit **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Example

The following example shows how to associate a policy map with a virtual template. In this example, the policy map named Parent is associated with the virtual template named VirtualTemplate1.

```
Router(config)# interface virtual-template1
Router(config-if)# service-policy output Parent
Router(config-if)# exit
Router(config)#
```

Applying the Virtual Template to an ATM Subinterface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe group-name**
4. **virtual-template template-number**
5. exit
6. interface atm number.subinterface [point-to-point]
7. pvc [name] vpi/vci
8. protocol pppoe group group-name
9. exit
10. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe group-name** **Example:** `Router(config)#` **bba-group pppoe group-name**	Creates a PPP over Ethernet (PPPoE) profile. Enters BBA group configuration mode. group-name is the name of the PPPoE profile.
Step 4	**virtual-template template-number** **Example:** `Router(config-bba-grp)#` **virtual-template template-number**	Associates a BBA group to the virtual template to be used for cloning virtual access interfaces. template-number is the identifying number of the virtual template.
Step 5	exit **Example:** `Router(config-bba-grp)# exit`	Exits BBA group configuration mode.
Step 6	interface atm number.subinterface [point-to-point] **Example:** `Router(config)# interface atm number.subinterface [point-to-point]`	Creates or modifies a subinterface. Enters subinterface configuration mode. atm is the interface type. number is the slot, module, and port number of the interface (for example 1/0/0). .subinterface is the number of the subinterface (for example, 1/0/0.1). (Optional) point-to-point indicates that the subinterface connects directly with another subinterface.

	Command or Action	Purpose
Step 7	pvc [name] vpi/vci **Example:** `Router(config-subif) pvc [name] vpi/vci`	Creates or modifies an ATM permanent virtual circuit (PVC). Enters ATM virtual circuit configuration mode. (Optional) name identifies the PVC and can contain up to 15 characters. vpi/ specifies the ATM network virtual path identifier (VPI) for this PVC. You must specify the slash. Valid values are from 0 to 255. The router treats a value that is outside the range of valid values as the connection ID. The default value is 0. **Note** The arguments vpi and vci cannot both be set to 0; if one is 0, the other cannot be 0. vci specifies the ATM network virtual channel identifier (VCI) for this PVC. Valid values are from 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. A value that is out of range causes an " unrecognized command" error message. The VCI value has local significance only and, therefore, is unique only on a single link, not throughout the ATM network. Typically, lower values from 0 to 31 are reserved for specific traffic (for example, F4 OAM, SVC signaling, ILMI, and so on) and should not be used.
Step 8	protocol pppoe group group-name **Example:** `Router(config-atm-vc)# protocol pppoe group group-name`	Enables PPP over Ethernet (PPPoE) sessions to be established on permanent virtual circuits (PVCs). group specifies a PPPoE profile (bba-group) to be used by PPPoE sessions on the interface. group-name is the name of the PPPoE profile (bba-group) to be used by PPPoE sessions on the interface. The group group-name points to the bba-group to be used for applying a virtual template interface with QoS policies to sessions.
Step 9	exit **Example:** `Router(config-atm-vc)# exit`	Exits ATM virtual circuit configuration mode.
Step 10	exit **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode.

Examples

The following example shows how to associate a virtual template interface with an ATM interface and apply the policies in the virtual template to the sessions on the interface. In the example, the service policy named Parent is applied to the Virtual-Template 8, which is associated with the bba-group named pppoeoa-group. The bba-group is applied to PVC 101/210 on ATM subinterface 4/0/1.10.

```
bba-group pppoe pppoeoa-group
Virtual-Template 8
interface ATM4/0/1.10 point-to-point
pvc 101/210
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
interface Virtual-Template8
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
ppp authentication chap
service-policy output Parent
```

Configuring PPP Session Queueing Using Radius

To configure PPPoEoA session queueing using RADIUS, perform the following configuration tasks:

- Configuring the Policy Map, page 73
- Adding the Cisco QoS AV Pairs to the RADIUS Profile, page 73

Configuring the Policy Map

The router allows you to use RADIUS to apply QoS policy maps to PPPoEoA sessions.

Adding the Cisco QoS AV Pairs to the RADIUS Profile

Cisco attribute-value (AV) pairs are vendor-specific attributes (VSAs) that allow vendors such as Cisco to support their own extended attributes. RADIUS attribute 26 is a Cisco VSA used to communicate vendor-specific information between the router and the RADIUS server.

The RADIUS user profile contains an entry for each user that the RADIUS server authenticates. Each entry establishes an attribute the user can access. When configuring PPPoEoA session queueing using RADIUS, enter the following Cisco AV-pair in the appropriate user profile:

```
Cisco-AVPair = "ip:sub-qos-policy-out=<name of egress policy>"
```

The Cisco AV-pair identifies the policy map the router is to use when applying QoS features to a PPPoEoA session. After receiving a service-logon request from the policy server, RADIUS sends a change of authorization (CoA) request to the router to activate the service for the user, who is already logged in. If the authorization succeeds, the router downloads the name of the policy map from RADIUS using the Cisco AV-pair and applies the QoS policy to the session.

Note Although the router also supports the RADIUS vendor specific attribute (VSA) 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the above attribute for QoS policy definitions.

Verifying PPP Session Queueing on ATM VCs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show policy-map [interface interface]**
4. show policy-map session [uid uid-number] [input | output [class class-name]]
5. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**show policy-map [interface interface]** **Example:** `Router# show policy-map [interface interface]`	Displays information about the policy map attached to the interface you specify. If you do not specify an interface, it displays information about all of the policy maps configured on the router. interface interface is the interface type and number (for example, atm 4/0/0).
Step 4	show policy-map session [uid uid-number] [input | output [class class-name]] **Example:** `Router# show policy-map session [uid uid-number] [input | output [class class-name]]`	Displays the QoS policy map in effect for subscriber sessions. (Optional) uid defines a unique session ID. (Optional) uid-number is a unique session ID. Valid values are from 1 to 65535. (Optional) input displays the upstream traffic of the unique session. (Optional) output displays the downstream traffic of the unique session. (Optional) class identifies the class that is part of the QoS policy-map definition. (Optional) class-name provides a class name that is part of the QoS policy-map definition.

	Command or Action	Purpose
Step 5	**show running-config** **Example:** `Router# show running-config`	Displays the running configuration on the router. The output shows the AAA setup and the configuration of the policy map, ATM VCs, PPPoEoA, dynamic bandwidth selection, virtual template, and RADIUS server.

Configuration Examples for PPP Session Queueing on ATM VCs

Example Configuring PPP Session Queueing on ATM VCs

The following example shows how to configure PPPoEoA session queueing. In the example, a hierarchical QoS policy named pm_hier2_0_2 is associated with Virtual-Template555, which is applied to the broadband aggregation group named pppoeoa-group.

```
bba-group pppoe pppoeoa-group
Virtual-Template 555
!
policy-map pm_hier2_child_0_2
class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
class cm_1
shape average percent 80
bandwidth remaining ratio 80
class class-default
shape average percent 50
bandwidth remaining ratio 20
policy-map pm_hier2_0_2
class class-default
shape average percent 100
bandwidth remaining ratio 100
service-policy pm_hier_child_0_2
interface ATM2/0/7.5555 point-to-point
pvc 1/5555
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
!
interface Virtual-Template555
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
ppp authentication chap
service-policy output pm_hier2_0_2
```

Example Configuring and Applying an Hierarchical Policy Map

Example Configuring and Applying an Hierarchical Policy Map, page 76 shows how to configure a hierarchical policy and apply it to a virtual template. The example contains a child policy map named child1 with QoS features defined for the gold and bronze traffic classes. The child1 policy is applied to the parent policy map, which is shaped to 512000 bps. The hierarchical policy is applied to the virtual template named virtual-template 1.

```
Router(config)# policy-map child1
Router(config-pmap)# class gold
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# class bronze
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 512000
Router(config-pmap-c)# service-policy child1
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface virtual-template 1
Router(config-if)# service-policy output parent
```

Example Setting Up RADIUS for PPP Session Queueing on ATM VCs

Example Setting Up RADIUS for PPP Session Queueing on ATM VCs, page 76 shows how to define the Cisco AV pairs used to download the policy map name to the router. The first three lines of a subscriber’s sample user profile contain the user password, service type, and protocol type. This information is entered into the subscriber’s user profile when the user profile is first created. The last line is an example of the Cisco QoS AV-pair added to the user profile. The policy map name downloaded to the router is p23.

```
userid    Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
cisco-avpair = "sub-qos-policy-out=p23"
```

Example Verifying PPP Session Queueing on ATM VCs

Example Verifying PPP Session Queueing on ATM VCs, page 76 uses the show pppoe session command to display the sessions established on the router. In this case, one session is active with a session ID (SID) of 6.

Displaying PPP Session Information--show pxf cpu queue session Command

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
Uniq ID    PPPoE    RemMAC    Port    VT    VA    State
    SID    LocMAC    VA-st    Type
    14    6    0009.b68d.bb37    ATM2/0/7.5555    555    Vi3.1    PTA
            0009.b68d.bc37    VC: 1/5555             UP
```

Example Verifying PPP Session Queueing on ATM VCs, page 76 uses the show policy-map session command to display QoS policy map statistics for traffic in the downstream direction. The example also shows the policy map configurations.

Displaying PPP Session Information--show policy-map session Command

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
Uniq ID    PPPoE    RemMAC    Port    VT    VA    State
    SID    LocMAC    VA-st    Type
    14    6    0009.b68d.bb37    ATM2/0/7.5555    555     Vi3.1     PTA
    0009.b68d.bc37 VC: 1/5555    UP
Router#
Router#
Router# show policy-map session uid 14
SSS session identifier 14 -
    Service-policy output: pm_hier2_0_2
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 50 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000
bandwidth remaining ratio 100
    Service-policy : pm_hier2_child_0_2
queue stats for all priority classes:
Queueing
priority level 1
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
Class-map: cm_0 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 0
0 packets, 0 bytes
30 second rate 0 bps
Priority: 0% (0 kbps), burst bytes 4470, b/w exceed drops: 0
Priority Level: 1
Police:
104000 bps, 1536 limit, 0 extended limit
conformed 0 packets, 0 bytes; action: transmit
exceeded 0 packets, 0 bytes; action: drop
violated 0 packets, 0 bytes; action: drop
Class-map: cm_1 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 1
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 237 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1600000, bc 6400, be 6400
target shape rate 1600000
bandwidth remaining ratio 80
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1000000, bc 4000, be 4000
target shape rate 1000000
```

```
bandwidth remaining ratio 20
Router# show policy-map pm_hier2_0_2
Policy Map pm_hier2_0_2
Class class-default
Average Rate Traffic Shaping
cir 100%
bandwidth remaining ratio 100
service-policy pm_hier2_child_0_2
Router# show policy-map pm_hier2_child_0_2
Policy Map pm_hier2_child_0_2
Class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
Class cm_1
Average Rate Traffic Shaping
cir 80%
bandwidth remaining ratio 80
Class class-default
Average Rate Traffic Shaping
cir 50%
bandwidth remaining ratio 20
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco QoS commands	*Cisco IOS Quality of Service Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PPP Session Queueing on ATM VCs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9 Feature Information for PPP Session Queueing on ATM VCs

Feature Name	Releases	Feature Information
PPP Session Queueing on ATM VCs	Cisco IOS XE Release 2.5	PPP Session Queueing on ATM Virtual Circuits (VCs) enables you to shape and queue PPP over Ethernet over ATM (PPPoEoA) sessions to a user specified rate. In Cisco IOS Release XE 2.5, this feature was introduced on the Cisco ASR 1000 series routers.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Traffic Policing

This feature module describes the Traffic Policing feature. The Traffic Policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligibility (DE) bit, IP precedence value, IP differentiated services code point (DSCP) value, MPLS experimental value, and Quality of Service (QoS) group.

Traffic policing allows you to control the maximum rate of traffic that is transmitted or received on an interface. The Traffic Policing feature is applied when a service-policy containing the feature is attached to an interface. A service-policy (traffic policy) is configured using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Traffic Policing

- Traffic policing can be configured on an interface or a subinterface.
- Traffic policing is not supported on the EtherChannel interfaces.

Benefits of Traffic Policing

Bandwidth Management Through Rate Limiting

Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface. Traffic policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most Traffic Policing configurations, traffic that falls within the rate parameters is transmitted, whereas traffic that exceeds the parameters is dropped or transmitted with a different priority.

Packet Marking

Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS). A packet is marked and these markings can be used to identify and classify traffic for downstream devices. In some cases, such as ATM Cell Loss Priority (CLP) marking or Frame Relay Discard Eligibility (DE) marking, the marking is used to decide whether the packet can be dropped in congested environments.

- Use traffic policing to set the IP precedence or DSCP values for packets entering the network. Networking devices within your network can then use the adjusted IP precedence values to determine how the traffic should be treated. For example, the Weighted Random Early Detection (WRED) feature uses the IP precedence values to determine the probability that a packet will be dropped.
- Use traffic policing to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets within the router.

Traffic can be marked without using the Traffic Policing feature. If you want to mark traffic but do not want to use Traffic Policing, see the "Marking Network Traffic" module.

Packet Prioritization for Frame Relay Frames

The Traffic Policing feature allows users to mark the Frame Relay DE bit of the Frame Relay frame. The Frame Relay DE bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, frames with the DE bit set to 1 are discarded before frames with the DE bit set to 0.

Packet Prioritization for ATM Cells

The Traffic Policing feature allows users to mark the ATM CLP bit in ATM cells. The ATM CLP bit is used to prioritize packets in ATM networks. The ATM CLP bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, cells with the ATM CLP bit set to 1 are discarded before cells with the ATM CLP bit set to 0.

How to Configure Traffic Policing

Configuring Traffic Policing

Command	Purpose
Router(config-pmap-c)# police bps burst-normal burst-max conform-action action exceed-action action violate-action action	Specifies a maximum bandwidth usage by a traffic class.

Monitoring and Maintaining Traffic Policing

Command	Purpose
Router# show policy-map	Displays all configured policy maps.
Router# show policy-map policy-map-name	Displays the user-specified policy map.
Router# show policy-map interface	Displays statistics and configurations of all input and output policies that are attached to an interface.

Configuration Examples for Traffic Policing

Example Configuring a Service Policy That Includes Traffic Policing

The following configuration shows how to define a traffic class (with the **class-map**command) and associate that traffic class with a traffic policy (with the **policy-map** command). Traffic policing is applied in the traffic policy. The **service-policy** command is then used to attach the traffic policy to the interface.

In this particular example, traffic policing is configured with the Committed Information Rate (CIR) at 8000 bits per second, the normal burst size at 2000 bytes, and the excess burst size at 4000 bytes. Packets coming into FastEthernet interface 1/1/1 are evaluated by the token bucket algorithm to analyze whether packets conform exceed, or violate the specified parameters. Packets that conform are transmitted, packets that exceed are assigned a QoS group value of 4 and are transmitted, and packets that violate are dropped.

```
Router(config)# class-map acgroup2
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map police
Router(config-pmap)# class acgroup2
Router(config-pmap-c)# police 8000 2000 4000 conform-action transmit exceed-action set-
qos-transmit 4 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/1/1
Router(config-if)# service-policy input police
Router(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Conceptual information about policing and shaping	"Policing and Shaping Overview" module
MQC	"Applying QoS Features Using the MQC" module
Marking network traffic	"Marking Network Traffic" module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2697	*A Single Rate Three Color Marker*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Traffic Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10 Feature Information for Traffic Policing

Feature Name	Releases	Feature Information
Traffic Policing	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. The following commands were modified: **police**, s**how policy-map**, **show policy-map interface**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Policer Enhancement Multiple Actions

Feature History

Release	Modification
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This document describes the Policer Enhancement Multiple Actions feature and includes the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

This feature further extends the functionality of the Cisco IOS XE single-rate policer and the Two-Rate Policer feature. The Traffic Policing and Two-Rate Policer features are traffic policing mechanisms that allow you to control the maximum rate of traffic sent or received on an interface. Both of these traffic policing mechanisms mark packets as either conforming to, exceeding, or violating a specified rate. After a packet is marked, you can specify an action to be taken on the packet based on that marking.

With both the Traffic Policing feature and the Two-Rate Policer feature, you can specify only one conform action, one exceed action, and one violate action. Now with the new Policer Enhancement Multiple Actions feature, you can specify multiple conform, exceed, and violate actions for the marked packets.

You specify the multiple actions by using the *action* argument of the **police** command. The resulting actions are listed in the table below.

Table 11 police Command Action Arguments

Specified Action	Result
drop	Drops the packet.
set-clp-transmit	Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet.
set-cos-transmit	Sets the Class of Service (CoS) value and transmits the packet.
set-discard-class-transmit	Sets the discard-class value and transmits the packet.
set-dscp-transmit *new-dscp*	Sets the IP differentiated services code point (DSCP) value and transmits the packet with the ATM CLP bit set to 1.
set-frde-transmit	Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet.
set-mpls-exp-transmit	Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits from 0 to 7 and transmits the packet.
set-mpls-exp-imposition-transmit	Sets the MPLS EXP bits from 0 to 7 at tag imposition and transmits the packet.
set-prec-transmit *new-prec*	Sets the IP Precedence level and transmits the packet.
set-qos-transmit *new-qos*	Sets the Quality of Service (QoS) group value and transmits the packet.
transmit	Transmits the packet.

Benefits

Before this feature, you could specify only *one* marking action for a packet, in addition to transmitting the packet. This feature provides enhanced flexibility by allowing you to specify *multiple* marking actions for a packet, as required. For example, if you know the packet will be transmitted through both a TCP/IP and a Frame Relay environment, you can change the DSCP value of the exceeding or violating packet, and also set the Frame Relay Discard Eligibility (DE) bit from 0 to 1 to indicate lower priority.

Restrictions

- Multiple policer actions can be configured on an interface, a subinterface, a Frame Relay data-link connection identifier (DLCI), and an ATM permanent virtual circuit (PVC) only.
- When using this feature, you can specify a maximum of four actions at one time.
- Multiple policer actions are not supported on EtherChannel interfaces.

Related Features and Technologies

- Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC)
- Class-Based Weighted Fair Queueing (CBWFQ)
- Class-Based Packet Marking
- Traffic Policing
- Two-Rate Policing

Related Documents

- "Applying QoS Features Using the MQC" module
- "Marking Network Traffic" module
- "Policing and Shaping Overview" module
- "Traffic Policing" module
- "Two-Rate Policer" module
- Cisco IOS Quality of Service Solutions Command Reference

Supported Standards MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CLASS-BASED-QOS-CAPABILITY-MIB

To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://www.cisco.com/go/mibs

RFCs

- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*

Prerequisites

- To configure the Policer Enhancement Multiple Actions feature, a traffic class and a service policy must be created, and the service policy must be attached to a specified interface.

Configuration Tasks

- Configuring Multiple Policer Actions, page 90
- Verifying the Multiple Policer Actions Configuration, page 90
- Troubleshooting Tips, page 90

Configuring Multiple Policer Actions

SUMMARY STEPS

1. Router(config)# **policy-map***policy-map-name*
2. Router(config-pmap)# **class***class-default*
3. Router(config-pmap-c)# **police** {**cir***cir*}[**bc** *conform-burst*]{**pir***pir*} [**be***peak-burst*] [**conform-action***action* [**exceed-action***action* [**violate-action** *action*]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **policy-map***policy-map-name*	Creates a policy map. Enters policy-map configuration mode.
Step 2	Router(config-pmap)# **class***class-default*	Specifies the default traffic class for a service policy. Enters policy-map class configuration mode.
Step 3	Router(config-pmap-c)# **police** {**cir***cir*}[**bc** *conform-burst*]{**pir***pir*} [**be***peak-burst*] [**conform-action***action* [**exceed-action***action* [**violate-action** *action*]]]	Configures traffic policing and specifies multiple actions applied to packets marked as conforming to, exceeding, or violating a specific rate. Use one line per action that you want to specify. Enters policy-map class police configuration mode.

Verifying the Multiple Policer Actions Configuration

Command	Purpose
`Router#` **show policy-map interface**	Displays statistics and configurations of all input and output policies attached to an interface.

Troubleshooting Tips

Check the interface type. Verify that this feature is supported on your interface. See the Restrictions, page 89.

Monitoring and Maintaining the Multiple Policer Actions

Command	Purpose
`Router#` **show policy-map**	Displays all configured policy maps.
`Router#` **show policy-map***`policy-map-name`*	Displays the user-specified policy map.
`Router#` **show policy-map interface**	Displays statistics and configurations of all input and output policies that are attached to an interface.

Configuration Examples

- Example Multiple Actions in a Two-Rate Policer, page 91
- Example Verifying the Multiple Policer Actions, page 91

Example Multiple Actions in a Two-Rate Policer

In the following example, a policy map called police is configured to use a two-rate policer to police traffic leaving an interface. Two rates, a committed information rate (CIR) of 1 Mbps and a peak information rate (PIR) of 2 Mbps, have been specified.

```
Router(config)# policy-map police
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 1000000 pir 2000000

Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action set-prec-transmit 4
Router(config-pmap-c-police)# exceed-action set-frde-transmit
Router(config-pmap-c-police)# violate-action set-prec-transmit 2
Router(config-pmap-c-police)# violate-action set-frde-transmit

Router(config-pmap-c-police)# end
```

The following actions will be performed on packets associated with the policy map called police:

- All packets marked as conforming to these rates (that is, packets conforming to the CIR) will be transmitted unaltered.
- All packets marked as exceeding these rates (that is, packets exceeding the CIR but not exceeding the PIR) will be assigned an IP Precedence level of 4, the DE bit will be set to 1, and then transmitted.
- All packets marked as violating the rate (that is, exceeding the PIR) will be assigned an IP Precedence level of 2, the DE bit will be set to 1, and then transmitted.

Example Verifying the Multiple Policer Actions

The following sample output of the **show policy-map**command displays the configuration for a service policy called police. In this service policy, multiple actions for packets marked as exceeding the specified CIR rate have been configured. For those packets, the IP Precedence level is set to 4, the DE bit is set to 1, and the packet is transmitted. Multiple actions for packets marked as violating the specified PIR rate have also been configured. For those packets, the IP Precedence level is set to 2, the DE bit is set to 1, and the packet is transmitted.

```
Router# show policy-map police
  Policy Map police
    Class class-default
     police cir 1000000 bc 31250 pir 2000000 be 31250
       conform-action transmit
       exceed-action set-prec-transmit 4
       exceed-action set-frde-transmit
       violate-action set-prec-transmit 2
       violate-action set-frde-transmit
```

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Control Plane Policing

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS XE routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Control Plane Policing

Output Rate-Limiting Support

Output rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to output control plane traffic with the **service-policy output** command. For more information, see the Output Rate-Limiting and Silent Mode Operation, page 96.

MQC Restrictions

The Control Plane Policing feature requires the MQC to configure packet classification, packet marking, and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing. Only two MQC actions are supported in policy maps--**police** and **set**.

Match Criteria Support and Restrictions

The following classification (match) criteria are supported:

- Standard and extended IP access control lists (ACLs).
- In class-map configuration mode, match criteria specified by the following commands:
    - **match dscp**
    - **match ip dscp**
    - **match ip precedence**
    - **match precedence**
    - **match protocol arp**
    - **match protocol ipv6**
    - **match protocol pppoe**

Note The **match protocol pppoe**command matches all PPPoE data packets that are sent to the control plane.

- ◦ **match protocol pppoe-discovery**

Note The **match protocol pppoe-discovery**command matches all PPPoE control packets that are sent to the control plane.

- ◦ **match qos-group**

Note The **match input-interface** command is not supported.

Note Features that require Network-Based Application Recognition (NBAR) classification may not work well at the control plane level.

Information About Control Plane Policing

Benefits of Control Plane Policing

Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches
- Ease of configuration for control plane policies
- Better platform reliability and availability

Control Plane Terms to Understand

On the Cisco ASR 1000 series router, the following terms are used for the Control Plane Policing feature.

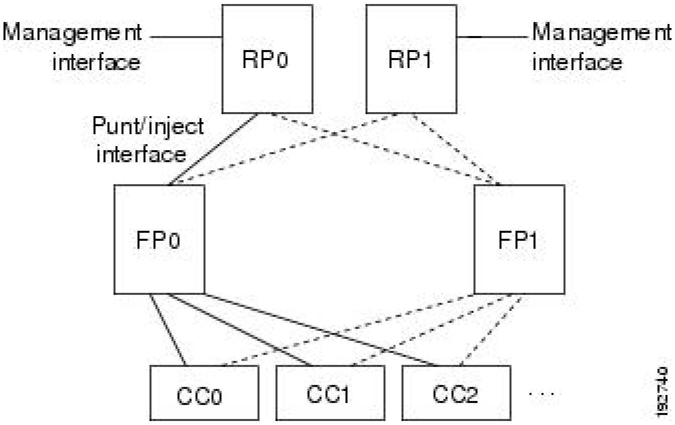
- Control plane (CP)--A collection of processes that run at the process level on the Route Processor (RP). These processes collectively provide high-level control for most Cisco IOS XE functions. The traffic sent to or sent by the control plane is called control traffic.
- Forwarding plane (FP)--A device that is responsible for high-speed forwarding of IP packets. Its logic is kept simple so that it can be implemented by hardware to do fast packet-forwarding. It punts packets that require complex processing (for example, packets with IP options) to the RP for the control-plane to process them.

Control Plane Policing Overview

To protect the CP on a router from DoS attacks and to provide fine-control over the traffic to or from the CP, the Control Plane Policing feature treats the CP as a separate entity with its own interface for ingress (input) and egress (output) traffic. This interface is called the punt/inject interface, and it is similar to a physical interface on the router. Along this interface, packets are punted from the FP to the RP (in the input direction) and injected from the RP to the FP (in the output direction). A set of quality of service (QoS) rules can be applied on this interface in order to achieve CoPP.

These QoS rules are applied only after the packet has been determined to have the CP as its destination or when a packet exits from the CP. You can configure a service policy (QoS policy map) to prevent unwanted packets from progressing after a specified rate limit has been reached; for example, a system administrator can limit all TCP/SYN packets that are destined for the CP to a maximum rate of 1 megabit per second.

Figure 1 Abstract Illustration of a Cisco ASR 1000 Series Router with Dual RPs and Dual FPs



The figure below provides an abstract illustration of a Cisco ASR 1000 series router with dual RPs and dual FPs. Only one RP and one FP are active at any time. The other RP and FP are in stand-by mode and do not receive traffic from the carrier card (CC). Packets destined to the CP come in through the carrier card, and then go through the active FP before being punted to the active RP. When an input QoS policy map is configured on the CP, the active FP performs the QoS action (for example, a transmit, drop, or set action) before punting packets to the active RP, in order to achieve the best protection of the control-plane in the active RP.

On the other hand, packets exiting the CP are injected to the active FP, and then go out through the carrier card. When an output QoS policy map is configured on the CP, the active FP performs the QoS action after receiving the injected packets from the RP. Again this saves the valuable CPU resource in the RP.

Note As shown in Control Plane Policing Overview, page 95, the management interface is directly connected to the RP, so all traffic through the management interface to or from the control-plane is not subject to the CoPP function performed by the FP.

In high-availability (HA) mode, when an RP switchover happens, the active FP forwards traffic to the new active RP along the new punt/inject interface. The active FP continues to perform the CoPP function before punting traffic to the new active RP. When an FP switchover happens, the new active FP receives traffic from the carrier card, and performs the CoPP function before punting traffic to the active RP.

Note The Cisco ASR 1000 series router handles some traditional control traffic in the FP directly to reduce the load on the CP. One example is the IP Internet Control Message Protocol (ICMP) echo-request packet sent to this router. When a Cisco ASR1000 series router receives such packets, the packets are handled directly in the FP without being punted to the RP. In order to be consistent with other Cisco routers and to provide the same capability to control such packets using CoPP, the Cisco ASR 1000 series router extends the CoPP function on such packets, even though the packets are not punted to the RP. Customers can still use the CoPP function to rate-limit or to mark such packets.

Output Rate-Limiting and Silent Mode Operation

A router is automatically enabled to silently discard packets when you configure output policing on control plane traffic using the **service-policy output** *policy-map-name* command.

Rate-limiting (policing) of output traffic from the CP is performed in silent mode. In silent mode, a router that is running Cisco IOS XE software operates without sending any system messages. If a packet that is exiting the control plane is discarded for output policing, you do not receive an error message.

How to Use Control Plane Policing

- Defining Control Plane Services, page 96
- Verifying Control Plane Services, page 98

Defining Control Plane Services

Perform this task to define CP services, such as packet rate control and silent packet discard, for the active RP.

Before you enter control-plane configuration mode to attach an existing QoS policy to the control plane, you must first create the policy using MQC to define a class map and policy map for control plane traffic.

Note

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Output policing does not provide any performance benefits. It simply controls the information that is leaving the device.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane**
4. **service-policy** {**input**| **output** *policy-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**control-plane** **Example:** `Router(config)# control-plane`	Enters control-plane configuration mode (a prerequisite for Defining Control Plane Services, page 96).

	Command or Action	Purpose
Step 4	**service-policy** {**input**| **output** *policy-map-name* **Example:** `Router(config-cp)# service-policy input control-plane-policy`	Attaches a QoS service policy to the control plane. Note the following points: • **input** --Applies the specified service policy to packets received on the control plane. • **output** --Applies the specified service policy to packets transmitted from the control plane and enables the router to silently discard packets. • *policy-map-name* --Name of a service policy map (created using the **policy-map** command) to be attached.

Step 5	**end**
	Example:
	`Router(config-cp)# end`
		(Optional) Returns to privileged EXEC mode.

Verifying Control Plane Services

SUMMARY STEPS

1. **enable**
2. **show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | output [class class-name]]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | output [class class-name]] **Example:** `Router# show policy-map control-plane all`	Displays information about the control plane. Note the following points: • **all** --(Optional) Service policy information about all QoS policies used on the CP. • **input** --(Optional) Statistics for the attached input policy. • **output** --(Optional) Statistics for the attached output policy. • **class** *class-name* --(Optional) Name of the traffic class whose configuration and statistics are displayed.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Examples

The following example shows that the policy map TEST is associated with the control plane. This policy map polices traffic that matches the class map TEST, while allowing all other traffic (that matches the class map "class-default") to go through as is.

```
Router# show policy-map control-plane

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
      20 packets, 11280 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 101
      police:
        8000 bps, 1500 limit, 1500 extended limit
        conformed 15 packets, 6210 bytes; action:transmit
        exceeded 5 packets, 5070 bytes; action:drop
        violated 0 packets, 0 bytes; action:drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
      105325 packets, 11415151 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
```

Configuration Examples for Control Plane Policing

- Example Configuring Control Plane Policing on Input Telnet Traffic, page 99
- Example Configuring Control Plane Policing on Output ICMP Traffic, page 100
- Example Marking Output Control Plane Packets, page 100

Example Configuring Control Plane Policing on Input Telnet Traffic

The following example shows how to apply a QoS policy on the CP for input Telnet traffic. Trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate.

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

! Allow
10.1.1.2
 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet

! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
```

```
Router(config)# class-map telnet-class

Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define control plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

Example Configuring Control Plane Policing on Output ICMP Traffic

The following example shows how to apply a QoS policy on the CP for egress ICMP port-unreachable packets. Trusted networks with source addresses 10.0.0.0 and 10.0.1.0 receive ICMP port-unreachable responses without constraint, while allowing all remaining ICMP port-unreachable responses to be dropped:

```
! Allow
10.0.0.0
 trusted network traffic.
Router(config)# access-list 141 deny icmp 10.0.0.0 0.0.0.255 any port-unreachable

! Allow
10.0.0.1
 trusted network traffic.
Router(config)# access-list 141 deny icmp 10.0.1.0 0.0.0.255 any port-unreachable

! Rate-limit all other ICMP traffic.
Router(config)# access-list 141 permit icmp any any port-unreachable
Router(config)# class-map icmp-class

Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# conform-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-out
Router(config-cp)# end
```

Example Marking Output Control Plane Packets

The following example shows how to apply a QoS policy on the CP to mark all egress IPv6 echo-request packets with IPv6 precedence 6.

```
! Match all IPv6 Echo Requests
Router(config)# ipv6 access-list coppacl-ipv6-icmp-request
Router(config-ipv6-acl)# permit icmp any any echo-request
Router(config-ipv6-acl)# exit
Router(config)# class-map match-all coppclass-ipv6-icmp-request
Router(config-cmap)# match access-group name coppacl-ipv6-icmp-request
Router(config-cmap)# exit
! Set all egress IPv6 Echo Requests with precedence 6
Router(config)# policy-map copp-policy
Router(config-pmap)# class coppclass-ipv6-icmp-request
Router(config-pmap-c)# set precedence 6
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define control plane service for the active route processor.
```

```
Router(config)# control-plane
Router(config-cp)# service-policy output copp-policy
Router(config-cp)# end
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
QoS features overview	"Quality of Service Overview" module
MQC	"Applying QoS Features Using the MQC" module
Security features overview	"Security Overview" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
• CISCO-CLASS-BASED-QOS-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Control Plane Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12 Feature Information for Control Plane Policing

Feature Name	Releases	Feature Information
Control Plane Policing	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2	The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. For Cisco IOS XE Release 2.1, this feature was implemented on Cisco ASR 1000 series routers. For Cisco IOS XE Release 2.2, this feature was modified to include support for packet marking, output rate-limiting, and additional match criteria. The following commands were introduced or modified: **match protocol pppoe**, **match protocol pppoe-discovery**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Class-Based Policing

Class-based policing allows you to control the maximum rate of traffic that is transmitted or received on an interface. Class-based policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Class-Based Policing

Class-Based Policing Functionality

The Class-Based Policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligibility (DE) bit, IP precedence value, IP differentiated services code point (DSCP) value, MPLS experimental value, and quality of service (QoS) group.

Class-based policing allows you to control the maximum rate of traffic transmitted or received on an interface. The Class-Based Policing feature is applied when you attach a traffic policy that contains the class-based policing configuration to an interface.

The Class-Based Policing feature works with a token bucket mechanism. There are currently two types of token bucket algorithms: a single token bucket algorithm and a two-token bucket algorithm. A single token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

Benefits of Class-Based Policing

Bandwidth Management Through Rate Limiting

Class-based policing allows you to control the maximum rate of traffic transmitted or received on an interface. Class-based policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most class-based policing configurations, traffic that falls within the rate parameters is transmitted, whereas traffic that exceeds the parameters is dropped or transmitted with a different priority.

Packet Marking

Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS). A packet is marked and these markings can be used to identify and classify traffic for downstream devices.

- Use class-based policing to set the IP precedence or DSCP values for packets entering the network. Networking devices within your network can then use the adjusted IP precedence values to determine how the traffic should be treated.
- Use class-based policing to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets.

Traffic can be marked without using the Class-Based Policing feature. If you want to mark traffic but do not want to use class-based policing, see the “Marking Network Traffic” module.

Restrictions for Class-Based Policing

Class-based policing can be configured on an interface or a subinterface, but it is not supported on EtherChannel or tunnel interfaces.

Restrictions for the Cisco ASR 903 Router

- Class-based policing on subinterfaces is not supported.
- Policing is supported for ingress policy maps only.
- Hierarchical policing (policing at both parent level and child level) is not supported.

How to Configure Class-Based Policing

- Configuring a Traffic Policing Service Policy, page 107
- Monitoring and Maintaining Traffic Policing, page 109
- Verifying Class-Based Traffic Policing, page 110

Configuring a Traffic Policing Service Policy

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match ip precedence** *precedence-value*
5. **exit**
6. **policy-map** *policy-map-name*
7. **class** {*class-name* | **class-default**}
8. **police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action*
9. **exit**
10. **exit**
11. **interface** *interface-type interface-number*
12. **service-policy** {**input** | **output**} *policy-map-name*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**class-map** [**match-all** | **match-any**] *class-map-name*
	Example:
	`Router(config)# class-map match-any MATCH_PREC`
		Specifies the name of the class map to be created and enters QoS class map configuration mode.
		• The class map defines the criteria to use to differentiate the traffic. For example, you can use the class map to differentiate voice traffic from data traffic, based on a series of match criteria defined using the **match** command.
		Note If the **match-all** or **match-any** keyword is not specified, traffic must match all the match criteria to be classified as part of the traffic class.

	Command or Action	Purpose
Step 4	**match ip precedence** *precedence-value* **Example:** `Router(config-cmap)# match ip precedence 0`	Enables packet matching on the basis of the IP precedence values you specify. **Note** You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Returns to global configuration mode.
Step 6	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map POLICE-SETTING`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters QoS policy-map configuration mode.

Step 7	**class** {*class-name* | **class-default**}
	Example:
	`Router(config-pmap)# class MATCH_PREC`
		Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy, and enters policy-map class configuration mode.

Step 8	**police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action* **Example:** `Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1 violate-action drop`	Configures traffic policing according to burst sizes and any optional actions specified.
Step 9	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Exits policy-map class configuration mode.
Step 10	**exit** **Example:** `Router(config-pmap)# exit`	(Optional) Exits QoS policy-map configuration mode.

	Command or Action	Purpose
Step 11	**interface** *interface-type interface-number* **Example:** `Router(config)# interface GigabitEthernet 0/0/1`	Configures an interface type and enters interface configuration mode. • Enter the interface type and interface number.
Step 12	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input POLICE-SETTING`	Attaches a policy map to an interface. • Enter either the **input** or **output** keyword and the policy map name.

Step 13	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring and Maintaining Traffic Policing

Note

SUMMARY STEPS

1. **enable**
2. **show policy-map**
3. **show policy-map** *policy-map-name*
4. **show policy-map interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show policy-map** **Example:** `Router# show policy-map`	Displays all configured policy maps.
Step 3	**show policy-map** *policy-map-name* **Example:** `Router# show policy-map pmap`	Displays the user-specified policy map.
Step 4	**show policy-map interface** **Example:** `Router# show policy-map interface`	Verifies that the Class-Based Policing feature is configured on your interface. If the feature is configured on your interface. • The command output displays policing statistics.

Verifying Class-Based Traffic Policing

Use the **show policy-map interface** command to verify that the Class-Based Policing feature is configured on your interface. If the feature is configured on your interface, the **show policy-map interface** command output displays policing statistics.

SUMMARY STEPS

1. **enable**
2. **show policy-map interface**
3. **show policy-map interface** *type interface*
4. **show policy-map interface** *type interface* **service instance** *service-instance number*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show policy-map interface** **Example:** `Router# show policy-map interface`	Verifies that the Class-Based Policing feature is configured on your interface. If the feature is configured on your interface. • The command output displays policing statistics.
Step 3	**show policy-map interface** *type interface* **Example:** `Router# show policy-map interface GigabitEthernet 0/0/1`	Displays traffic statistics for policies applied to a specific interface.
Step 4	**show policy-map interface** *type interface* **service instance** *service-instance number* **Example:** `Router# show policy-map interface GigabitEthernet 0/0/1 service instance 1`	Displays the policy map information for a given service instance under a port channel.
Step 5	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Example: Verifying Class-Based Traffic Policing

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

- Troubleshooting Tips, page 111

Troubleshooting Tips

Check the interface type. Verify that class-based policing is supported on your interface. See the Restrictions for Class-Based Policing, page 106.

Configuration Examples for Class-Based Policing

Example Configuring a Service Policy That Includes Traffic Policing

In the following example, class-based policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving the interface.

```
class-map access-match
 match access-group 1
 exit
policy-map police-setting
 class access-match
  police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
  exit
 exit
 service-policy output police-setting
```

The treatment of a series of packets leaving FastEthernet interface 1/1/1 depends on the size of the packet and the number of bytes remaining in the conform and exceed token buckets. The series of packets are policed based on the following rules:

- If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T - T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket. The token arrival rate is calculated as follows:

(time between packets < which is equal to T - T1 > * policer rate)/8 bytes

- If the number of bytes in the conform bucket is greater than the length of the packet (for example, B), then the packet conforms and B bytes should be removed from the bucket. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in the conform bucket is less than the length of the packet, but the number of bytes in the exceed bucket is greater than the length of the packet (for example, B), the packet exceeds and B bytes are removed from the bucket.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet, and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket ((0.25 * 8000)/8), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size, is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken, and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket).

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets ((.40 * 8000)/8). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket, and 200 bytes overflow the conform token bucket (because only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet, and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket ((.20 * 8000)/8). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Verifying Class-Based Traffic Policing

Use the **show policy-map interface** command to verify that the Class-Based Policing feature is configured on your interface. If the feature is configured on your interface, the **show policy-map interface** command output displays policing statistics:

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

Use the **show policy-map interface** *type nummber* command to view the traffic statistics for policies applied to that specific interface:

```
Router# show policy-map interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1

  Service-policy input: TUNNEL_MARKING

    Class-map: MATCH_PREC (match-any)
      72417 packets, 25418367 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      QoS Set
        ip precedence tunnel 3
          Marker statistics: Disabled

    Class-map: MATCH_DSCP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp default (0)
      QoS Set
        ip dscp tunnel 3
          Marker statistics: Disabled

    Class-map: class-default (match-any)
      346462 packets, 28014400 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

  Service-policy output: POLICE-SETTING
```

```
    Class-map: MATCH_PREC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      police:
          cir 8000 bps, bc 1000 bytes, be 1000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          set-qos-transmit 1
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps, violate 0000 bps

    Class-map: class-default (match-any)
      31 packets, 2019 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

Use the **show policy-map interface service instance** command to view the traffic statistics for policies applied to that specific interface:

```
Router# show policy-map interface gigabitethernet 0/0/1 service instance 1
    Service-policy input: p

    Class-map: prec1 (match-all)
            0 packets, 0 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: ip precedence 1
            police:
                            cir 10000000 bps, bc 312500 bytes
                    conformed 0 packets, 0 bytes; actions:
                            transmit
                    exceeded 0 packets, 0 bytes; actions:
                            drop
                    conformed 0000 bps, exceeded 0000 bps

    Class-map: class-default (match-any)
            0 packets, 0 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: any
```

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Traffic marking	“Marking Network Traffic” module
Traffic policing	“Traffic Policing” module
Traffic policing and shaping concepts and overview information	“Policing and Shaping Overview”
Modular Quality of Service Command-Line Interface (MQC)	“Applying QoS Features Using the MQC” module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
Class-Based Quality of Service MIB • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2697	*A Single Rate Three Color Marker*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Class-Based Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13 Feature Information for Class-Based Policing

Feature Name	Releases	Feature Information
Class-Based Policing	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	This feature was introduced on Cisco ASR 1000 Series Routers. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router. The following command was introduced or modified: **police**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

QoS Percentage-Based Policing

The QoS: Percentage-Based Policing feature allows you to configure traffic policing on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About QoS Percentage-Based Policing

Benefits for QoS Percentage-Based Policing

This feature provides the ability to configure traffic policing on the basis of a percentage of bandwidth available on an interface, and it allows you to specify burst sizes in milliseconds. Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. That is, you do not have to recalculate the bandwidth for each interface or configure a different policy map for each type of interface.

Configuration of Class and Policy Maps for QoS Percentage-Based Policing

To configure the QoS: Percentage-Based Policing feature, you must define a traffic class, configure a policy map, and then attach that policy map to the appropriate interface.

The MQC is a command-line interface that allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach these traffic policies to interfaces.

In the MQC, the **class-map** command is used to define a traffic class (which is then associated with a traffic policy). The purpose of a traffic class is to classify traffic.

The MQC consists of the following three processes:

- Defining a traffic class with the **class-map** command.
- Creating a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).
- Attaching the traffic policy to the interface with the **service-policy** command.

A traffic class contains three major elements: a name, a series of match commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands (that is, match-all or match-any). The traffic class is named in the **class-map** command line; for example, if you enter the **class-map cisco** command while configuring the traffic class in the CLI, the traffic class would be named "cisco".

The **match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

Traffic Regulation Mechanisms and Bandwidth Percentages

Cisco IOS XE quality of service (QoS) offers two kinds of traffic regulation mechanisms--traffic policing and traffic shaping. A traffic policer typically drops traffic that violates a specific rate. A traffic shaper typically delays excess traffic using a buffer to hold packets and shapes the flow when the data rate to a queue is higher than expected.

Traffic shaping and traffic policing can work in tandem and can be configured in a class map. Class maps organize data packets into specific categories ("classes") that can, in turn, receive a user-defined QoS treatment when used in policy maps (sometimes referred to as "service policies").

Before this feature, traffic policing and traffic shaping were configured on the basis of a user-specified amount of bandwidth available on the interface. Policy maps were then configured on the basis of that specific amount of bandwidth, meaning that separate policy maps were required for each interface.

This feature provides the ability to configure traffic policing on the basis of a percentage of bandwidth available on the interface. Configuring traffic policing in this manner enables customers to use the same policy map for multiple interfaces with differing amounts of bandwidth.

Configuring traffic policing on the basis of a percentage of bandwidth is accomplished by using the **police** (percent) and **shape** (percent) commands.

Burst Size in Milliseconds Option

The purpose of the burst parameters (bc and be) is to drop packets gradually and to avoid tail drop. Setting sufficiently high burst values helps to ensure good throughput.

This feature allows you the option of specifying the committed burst (bc) size and the extended burst (be) as milliseconds (ms) of the class bandwidth when you configure traffic policing. The number of milliseconds is used to calculate the number of bytes that will be used by the QoS: Percentage-Based Policing feature.

Specifying these burst sizes in milliseconds is accomplished by using the **bc** and **be** keywords (and their associated arguments) of the **police** (percent) and **shape** (percent) commands.

How to Configure QoS Percentage-Based Policing

Configuring a Class and Policy Map for Percentage-Based Policing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name*| **class-default**}
5. **police cir percent** *percentage* [*burst-in-ms*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percent*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**policy-map** *policy-name*
	Example:
	`Router(config)# policy-map`
	`policy1`
		Specifies the name of the policy map to be created. Enters policy-map configuration mode.
		• Enter the policy map name.

Step 4	**class** {*class-name*| **class-default**}
	Example:
	`Router(config-pmap)# class class1`
		Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.
		• Enter the class name or specify the default class (class-default).

Step 5	**police cir percent** *percentage* [*burst-in-ms*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percent*] **Example:** `Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40`	Configures traffic policing on the basis of the specified bandwidth percentage and optional burst sizes. Enters policy-map class police configuration mode. • Enter the bandwidth percentage and optional burst sizes.

Step 6	**end**
	Example:
	`Router(config-pmap-c-police)# end`
		Exits policy-map class police configuration mode.

Attaching the Policy Map to an Interface for Percentage-Based Policing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**interface** *type number*
	Example:
	`Router(config)#`
	`interface serial4/0/0`
		Configures an interface (or subinterface) type and enters interface configuration mode.
		• Enter the interface type number.
		Note Depending on the needs of your network, you may need to attach the policy map to a subinterface, an ATM PVC, a Frame Relay DLCI, or other type of interface.

Step 4	**pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	(Optional) Creates or assigns a name to an ATM PVC and specifies the encapsulation type on an ATM PVC. Enters ATM VC configuration mode. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, skip this step and proceed with Attaching the Policy Map to an Interface for Percentage-Based Policing, page 120.

Step 5	**service-policy** {**input**| **output**} *policy-map-name*
	Example:
	`Router(config-if)#`
	`service-policy input policy1`
	Example:
		Specifies the name of the policy map to be attached to the input or output direction of the interface.
		Note Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
		• Enter the policy map name.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Exits interface configuration mode.

Verifying the Percentage-Based Policing Configuration

SUMMARY STEPS

1. **enable**
2. **show class-map** [*class-map-name*]
3.
4. **show policy-map interface** *interface-name*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** [*class-map-name*] **Example:** `Router# show class-map class1`	Displays all information about a class map, including the match criterion. • Enter class map name.
Step 3		

Step 4	**show policy-map interface** *interface-name*
	Example:
	`Router#`
	`show policy-map interface serial4/0/0`
		Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		• Enter the interface name.

Step 5	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

- Troubleshooting Tips for Percentage-Based Policing, page 122

Troubleshooting Tips for Percentage-Based Policing

The commands in the Verifying the Percentage-Based Policing Configuration, page 122 section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If, after using the **show** commands listed above, you find that the configuration is not correct or the feature is not functioning as expected, perform these operations:

If the configuration is not the one you intended, complete the following procedures:

1. Use the **show running-config** command and analyze the output of the command.
2. If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
3. Attach the policy map to the interface again.

If the packets are not being matched correctly (for example, the packet counters are not incrementing correctly), complete the following procedures:

1. Run the **show policy-map**command and analyze the output of the command.
2. Run the **show running-config** command and analyze the output of the command.
3. Use the **show policy-map interface** command to verify that the policy map is attached to the interface and that the committed information rate (CIR) has been calculated on the basis of the percentage of the interface bandwidth.

Configuration Examples for QoS Percentage-Based Policing

Example Specifying Traffic Policing on the Basis of a Bandwidth Percentage

The following example configures traffic policing using a CIR and a peak information rate (PIR) on the basis of a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40

Router(config-pmap-c-police)# end
```

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example.

```
Router> enable
Router# configure terminal
Router(config-if)#

interface serial4/0/0
Router(config-if)#

service-policy input policy1
Router(config-if)# end
```

Example Verifying the Percentage-Based Policing Configuration

This section contains sample output from the **show policy-map interface** command and the **show policy-map** command. The output from these commands can be used to verify and monitor the feature configuration on your network.

The following is sample output from the **show policy-map** command. This sample output displays the contents of a policy map called "policy1." In policy 1, traffic policing on the basis of a CIR of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
       conform-action transmit
       exceed-action drop
       violate-action drop
```

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed burst (bc) and excess burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0
 Serial2/0/0
  Service-policy output: policy1 (1050)
    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
          pir 819000 bps, be 40960 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
    Class-map: class-default (match-any) (1054/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1055)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bytes.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

Formula for Calculating the CIR

When calculating the CIR, the following formula is used:

CIR percentage specified (as shown in the output of the **show policy-map**command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

On serial interface 2/0, the bandwidth (BW) is 2048 kbps. To see the bandwidth of the interface, use the **show interfaces** command. A sample is shown below:

```
Router# show interfaces serial2/0/0
```

```
Serial2/0/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CI:

20 % * 2048 kbps = 409600 bps

Formula for Calculating the PIR

When calculating the PIR, the following formula is used:

PIR percentage specified (as shown in the output of the **show policy-map**command) * bandwidth (BW) of the interface (as shown in the output of the **show interfaces** command) = total bits per second

On serial interface 2/0/0, the bandwidth (BW) is 2048 kbps. To see the bandwidth of the interface, use the **show interfaces** command. A sample is shown below:

```
Router# show interfaces serial2/0
Serial2/0/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

Note Discrepancies between this total and the total shown in the output of the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

Formula for Calculating the Committed Burst (bc)

When calculating the bc, the following formula is used:

The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

(300 ms * 409600 bps) / 8 = 15360 bytes

Formula for Calculating the Excess Burst (be)

When calculating the bc and the be, the following formula is used:

The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Modular QoS Command-Line Interface (CLI) (MQC), including information about attaching policy maps	"Applying QoS Features Using the MQC" module
Traffic shaping and traffic policing	"Policing and Shaping Overview" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2697	*A Single Rate Three Color Marker*
RFC 2698	*A Two Rate Three Color Marker*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for QoS Percentage-Based Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14 Feature Information for QoS: Percentage-Based Policing

Feature Name	Releases	Feature Information
QoS: Percentage-Based Policing	Cisco IOS XE Release 2.1	The QoS: Percentage-Based Policing feature allows you to configure traffic policing and traffic shaping on the basis of a percentage of bandwidth available on the interface. This feature also allows you to specify the committed burst (bc) size and the excess burst (be) size (used for configuring traffic policing) in milliseconds (ms). Configuring traffic policing in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth. This feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **police (percent)**, **shape (percent)**, **show policy-map**, **show policy-map interface**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Two-Rate Policer

This module describes the Two-Rate Policer feature and explains how to configure it.

History for the Two-Rate Policer Feature

Release	Modification
Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.

Finding Support Information for Cisco IOS XE Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE Software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

Networks police traffic by limiting the input or output transmission rate of a class of traffic based on user-defined criteria. Policing traffic allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or class of service (CoS).

The Two-Rate Policer performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the IP precedence value, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, Quality of Service (QoS) group, ATM Cell Loss Priority (CLP) bit, and the Frame Relay Discard Eligibility (DE) bit.

With the Two-Rate Policer, you can enforce traffic policing according to two separate rates--committed information rate (CIR) and peak information rate (PIR). You can specify the use of these two rates, along with their corresponding values, by using two keywords, **cir** and **pir**, of the **police** command.

The Two-Rate Policer manages the maximum rate of traffic through a token bucket algorithm. The token bucket algorithm can use the user-configured values to determine the maximum rate of traffic allowed on an interface at a given moment in time. The token bucket algorithm is affected by all traffic entering or leaving the interface (depending on the location of the interface on which the Two-Rate Policer is configured) and is useful in managing network bandwidth in cases where several large packets are sent in the same traffic stream.

Three Policing Actions

The token bucket algorithm provides users with three actions for each packet: a conform action, an exceed action, and a violate action. Traffic entering the interface with Two-Rate Policer configured is placed in to one of these categories. Within these three categories, users can decide packet treatments. For instance, packets that conform can be configured to be sent, packets that exceed can be configured to be sent with a decreased priority, and packets that violate can be configured to be dropped.

The Two-Rate Policer is often configured on interfaces at the edge of a network to limit the rate of traffic entering or leaving the network. In the most common configurations, traffic that conforms is sent and traffic that exceeds is sent with a decreased priority or is dropped. Users can change these configuration options to suit their network needs.

Note Additionally, the Two-Rate Policer enables you to implement Differentiated Services (DiffServ) Assured Forwarding (AF) Per-Hop Behavior (PHB) traffic conditioning.

Replenishment Functionality

The conforming bucket is replenished at the CIR and the exceeding bucket is replenished at the PIR. The PIR must be greater than the CIR.

When a packet arrives, the system checks to see if there are enough tokens in the conforming and the exceeding bucket to cover that packet. If there are enough tokens in both buckets, the conforming action is taken and the amount of tokens required to transmit a conforming packet is removed from both the conforming and exceeding buckets.

If the conforming bucket does not contain enough tokens to cover the packet, but the exceeding bucket does contain enough tokens, the exceeding action is taken. In this case, the system removes the appropriate number of tokens from the exceeding bucket only.

If there are not enough tokens in the exceeding bucket to cover the packet, the violating action is taken.

- Benefits of Two-Rate Policing, page 131
- Restrictions for Two-Rate Policing, page 131

Benefits of Two-Rate Policing

Bandwidth Management Through Rate Limiting

This feature provides improved bandwidth management through rate limiting. Before this feature was available, you could police traffic with the single-rate Traffic Policing feature. The Traffic Policing feature provided a certain amount of bandwidth management by allowing you to set the peak burst size (be). The Two-Rate Policer supports a higher level of bandwidth management and supports a sustained excess rate. With the Two-Rate Policer, you can enforce traffic policing according to two separate rates--CIR and PIR--specified in bits per second (bps).

Packet Marking Through the Precedence, the DSCP Value, the MPLS Experimental Value, and the QoS Group Setting

In addition to rate-limiting, the Two-Rate Policer allows you to independently mark the packet according to whether the packet conforms, exceeds, or violates a specified rate. Packet marking also allows you to partition your network into multiple priority levels or classes of service (CoS).

- Use the Two-Rate Policer to set the IP precedence value, the IP DSCP value, or the MPLS experimental value for packets that enter the network. Then networking devices within your network can use the this setting to determine how the traffic should be treated. For example, the Weighted Random Early Detection (WRED) feature uses the IP precedence value to determine the probability that a packet will be dropped.
- Use the Two-Rate Policer to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets within the router.

If you want to mark traffic but do not want to use the Two-Rate Policer, see the "Marking Network Traffic" module.

Packet Marking for Frame Relay Frames

The Two-Rate Policer allows users to mark the Frame Relay DE bit of the Frame Relay frame. The Frame Relay DE bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, frames that have the DE bit set to 1 are discarded before frames that have the DE bit set to 0.

Packet Marking for ATM Cells

The Two-Rate Policer allows users to mark the ATM CLP bit in ATM cells. The ATM CLP bit is used to prioritize packets in ATM networks. The ATM CLP bit is one bit and, therefore, can be set to either 0 or 1. In congested environments, cells that have the ATM CLP bit set to 1 are discarded before cells that have the ATM CLP bit set to 0.

Restrictions for Two-Rate Policing

The following restrictions apply to the Two-Rate Policer:

- Two-rate policing can be configured on an interface, a subinterface, a Frame Relay data-link connection identifier (DLCI), and an ATM permanent virtual circuit (PVC).
- Two-rate policing is not supported on EtherChannel or tunnel interfaces.

Prerequisites for Two-Rate Traffic Policing

To configure the Two-Rate Policer, a traffic class and a service policy must be created, and the service policy must be attached to a specified interface.

Configuration Tasks

See the following sections for configuration tasks for the Two-Rate Policer feature.

- Configuring the Two-Rate Policer, page 132
- Verifying the Two-Rate Policer Configuration, page 133
- Troubleshooting Tips, page 133

Configuring the Two-Rate Policer

Command	Purpose

`Router(config-pmap-c)#`
police cir
`cir [`**bc***`conform-burst`*
`]` **pir** *`pir`*
`[`**be***`peak-burst`*
`]`
`[`**conform-action** *action*
`[`**exceed-action** *action*
`[`**violate-action** *action*`]]]`
	Specifies that both the CIR and the PIR are to be used for two-rate traffic policing, and specifies multiple actions applied to packets marked as conforming to, exceeding, or violating a specific rate. Use one line per action that you want to specify. Enters policy-map class police configuration mode.
	The **bc** and **be** keywords and their associated arguments (*conform-burst* and *peak-burst* , respectively) are optional.

Although not required for configuring the Two-Rate Policer, the command syntax of the **police** command also allows you to specify the action to be taken on a packet when you enable an optional *action* argument. The resulting action corresponding to the keyword choices are listed in Table 1 .

Table 15 police Command Action Keywords

Keyword	Resulting Action
drop	Drops the packet.
set-clp-transmit	Sets the ATM CLP bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.
set-dscp-transmit *new-dscp*	Sets the IP DSCP value and sends the packet with the new IP DSCP value setting.
set-frde-transmit	Sets the Frame Relay DE bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.

Keyword	Resulting Action
set-mpls-exp-transmit	Sets the MPLS experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.
set-prec-transmit *new-prec*	Sets the IP precedence and sends the packet with the new IP precedence value setting.
set-qos-transmit *new-qos*	Sets the QoS group value and sends the packet with the new QoS group value setting.
transmit	Sends the packet with no alteration.

Verifying the Two-Rate Policer Configuration

Command	Purpose
`Router#` **show policy-map interface**	Displays statistics and configurations of all input and output policies attached to an interface.

Troubleshooting Tips

Monitoring and Maintaining the Two-Rate Policer

Command	Purpose
`Router#` **show policy-map**	Displays all configured policy maps.
`Router#` **show policy-map***`policy-map-name`*	Displays the user-specified policy map.
`Router#` **show policy-map interface**	Displays statistics and configurations of all input and output policies that are attached to an interface.

Configuration Examples

This section provides the following configuration example:

- Example Limiting the Traffic Using a Policer Class, page 134

Example Limiting the Traffic Using a Policer Class

In this example, the Two-Rate Policer is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
 transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config)# interface serial3/0/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic exceeding 1 Mbps will be dropped. The burst parameters are set to 10,000 bytes.

In the following example, 1.25 Mbps of traffic is sent ("offered") to a *policer* class.

```
Router# show policy-map interface serial3/0/0
 Serial3/0/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

The Two-Rate Policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

Additional References

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*

Related Topic	Document Title
Token bucket mechanisms	"Policing and Shaping Overview" module
MQC	"Applying QoS Features Using the MQC" module
QoS features such traffic marking, and traffic policing	• "Marking Network Traffic" module • "Traffic Policing" module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2698	*A Two Rate Three Color Marker*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.